AD-A373756

DTIC-BRR-TR-03--2000

DTIC

Information for the Defense Community

The DTIC® Review

INFORMATION TERRORISM

Unclassified/Unlimited

20000301070

Vol. 5, No. 1
March 2000

The DTIC Review is published by the
Defense Technical Information Center (DTIC),
DTIC-BRR, 8725 John J. Kingman Road, Suite 0944
Ft. Belvoir, VA 22060-6218
Telephone: (703)767-8266, DSN 427-8266
FAX: (703) 767-9070, DSN 427-9070
Email: bibs@dtic.mil

Opinions expressed herein are those of the authors and do not necessarily reflect those of the Department of Defense or its elements.

Editorial Staff
Editor: Christian M. Cupp
Compiler and Research Advisor: Phyllis Levine
Composition Editor: Diana Elkins

Distribution *The DTIC Review* is approved for public release.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY) 03-2000	2. REPORT TYPE Final	3. DATES COVERED (From - To) March 2000

4. TITLE AND SUBTITLE

The DTIC Review

Information Terrorism

Vol. 5 No. 1

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Cupp, Christian M.; Editor

Levine, Phyllis ; Compiler

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-BRR
8725 John J. Kingman Rd, Suite 0944
Ft.Belvoir, VA 22060-6218

8. PERFORMING ORGANIZATION REPORT NUMBER

DTIC-BRR-TR-03--2000

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-BRR
8725 John J. Kingman Rd, Suite 0944
Ft.Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

A - Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

This publication is published irregularly by the Defense Technical Information Center.

14. ABSTRACT

The information revolution has had a dramatic impact on every aspect of our lives. Commercial activities, all the way from the world's financial markets to the most basic purchases in stores, are driven by the changes in information technology. It is, therefore, not surprising that military operations are equally bound by these technologies which, at first glance, seem so remote from the world of troop movements and combat. But, in fact, these technologies are changing not only society but also our definition of war and the conduct of military operations. Throughout history, military doctrine, organization and strategy have continually undergone profound, technology-driven changes.

Modern warfare, unlike that of past epochs, is "information intensive," meaning the conduct of effective military operations requires a greater accumulation of data than ever before. Today, access to information is just as crucial as possession of petroleum, oil, lubricants, and ammunition. Cyberwar refers to conducting military operations according to information-related principles. It means disrupting or destroying information and communications systems. It means trying to know everything about an adversary while keeping the adversary from knowing much about oneself.

15. SUBJECT TERMS

Information Warfare, Cyberwar, Cyber attacks, Netwar, Electronic Warfare, Tactical Data Systems, Threat Evaluation, Unconventional Warfare

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Phyllis Levine
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED	Unclassified Unlimited		19b. TELEPHONE NUMBER (include area code) 703-767-8266

The DTIC® Review

Information Terrorism

AD-A 373756

Vol. 5, No. 1
March, 2000

FOREWORD

The information revolution has had a dramatic impact on every aspect of our lives. It is, therefore, not surprising that military operations are equally bound by these technologies which, at first glance, seem so remote from the world of troop movements and combat. But, in fact, these technologies are changing not only society but also our definition of war and the conduct of military operations.

This edition of The DTIC Review focuses on our current definition of war and the conduct of military operations in our present information intensive environment.

The editorial staff hope you find this effort of value and appreciate your comments.

Kurt N. Molholm
Administrator

TABLE OF CONTENTS

INTRODUCTION

The information revolution has had a dramatic impact on every aspect of our lives. Commercial activities, all the way from the world's financial markets to the most basic purchases in stores, are driven by the changes in information technology. It is, therefore, not surprising that military operations are equally bound by these technologies which, at first glance, seem so remote from the world of troop movements and combat. But, in fact, these technologies are changing not only society but also our definition of war and the conduct of military operations. Throughout history, military doctrine, organization and strategy have continually undergone profound, technology-driven changes.

Modern warfare, unlike that of past epochs, is "information intensive," meaning the conduct of effective military operations requires a greater accumulation of data than ever before. Today, access to information is just as crucial as possession of petroleum, oil, lubricants, and ammunition.

According to a recent analysis, there are hundreds of thousands of "attacks" against military information systems each year and, while almost all of these penetration efforts have been by so-called "hackers," and although nearly all have failed, the few that have been successful raise troubling prospects. Possession of one valid ID and password leads to the exposure of other, presumably better-protected, sites. A breakdown in network security at any point may facilitate access into the entire system.

A computer system's vulnerability is compounded by the fact that attacks against it are likely to be staged from a remote point. Through manipulation of a telephone system and skillful use of a computer, a distant and unseen attacker can cause incalculable damage with little likelihood of being identified.

Cyberwar refers to conducting military operations according to information-related principles. It means disrupting or destroying information and communications systems. It means trying to know everything about an adversary while keeping the adversary from knowing much about oneself. It means turning the "balance of information and knowledge" in one's favor, especially if the balance of forces is not. It means using knowledge so that less capital and labor may have to be expended.

Cyberwar has broad ramifications for military organization and doctrine. Moving to networked structures may require some decentralization of command and control. Decentralization is only part of the picture. New technology may also provide greater "topsight," a central understanding of the big picture that enhances the management of complexity. This pairing of decentralization with topsight brings the real gains.

The selected documents and bibliography are a representation of the material available on information terrorism from DTIC's extensive collection. Additional references, including electronic resources, can be found at the end of the volume. In-depth literature searches may be requested by contacting the Reference and Retrieval Services Branch at the Defense Technical Information Center: (703) 767-8274/DSN 427-8274;
FAX (703) 767-9070; E-mail bibs@dtic.mil

DOCUMENT 1

The Department of Defense and the Age Of Information Operations

AD-A345602

1998

U.S. Army War College
Carlisle Barracks, Pennsylvania

STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

THE DEPARTMENT OF DEFENSE AND THE AGE OF INFORMATION OPERATIONS

BY

LIEUTENANT COLONEL ALAN T. EVANS
United States Air Force

USAWC CLASS OF 1998

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

THE DEPARTMENT OF DEFENSE AND THE AGE OF INFORMATION OPERATIONS

by

Lt Col Alan T. Evans

Col Brian D. Moore, USMC, Ret.
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Alan T. Evans, Lt Col, United States Air Force

TITLE: THE DEPARTMENT OF DEFENSE AND THE AGE OF INFORMATION OPERATIONS

FORMAT: USAWC Strategy Research Project

DATE: 13 May 1998 PAGES: 24 CLASSIFICATION: U

This paper explains the challenges and vulnerabilities the Nation and especially the military will face in the next century as our dependence on information systems and associated infrastructure continues to grow. It will highlight the results of the President's Commission on Critical Infrastructure Protection and discuss the steps necessary to protect the information systems upon which we have come to so heavily depend. It will highlight that without a comprehensive national policy in protecting information infrastructures poses a great risk to its military, commercial users and ultimately the Nation.

TABLE OF CONTENTS

LIST OF TABLES

INTRODUCTION

> There are some who believe we are going to have an electronic Pearl Harbor, so to speak, before we really make [computer security] the kind of priority that many of us believe it deserves to be made. Do you think we're going to need that kind of real awakening?
>
> —Sen. Sam Nunn

> I don't know whether we will face an electronic Pearl Harbor, but we will have, I'm sure some very unpleasant circumstances. I'm certainly very well prepared to predict some very, very large and uncomfortable incidents.
>
> —CIA Director John M. Deutch

[Testimonies before the U.S. Senate Committee on Government Affairs, Subcommittee for Permanent Investigations, Vulnerability of United States Government Information Systems to Computer Attacks, Hearings, June 25, 1996.][1]

As the United States emerges from the Industrial to the Information Age our nation increases its vulnerabilities in the cyber dimension. Cyber War is defined as a comprehensive information-oriented approach to battle that may be to the information age what blitzkrieg was to the industrial age.[2] This is a global phenomenon with a multipolar world that relies on international finance, banking, worldwide commerce and communication networks. This digital interdependency creates many liabilities as well. It is becoming more and more apparent that government and industry are not prepared to respond to the Information Operations threat. The anonymity of the attacker forces one to take precautions on many fronts. Data streams on the Internet do not declare themselves at customs when they enter a country. The problem is that we do not know if it is an employee that forgets their password and tries to get back into the system, a student trying to hack into a network, a competitor or even an enemy nation-state with hostile intentions. The intertwined nature of the information age is altering the nature of social conflict. The new telecommunications technologies are enabling small nongovernmental players to organize into well-coordinated networks.[3] The cyber attack threat against the United States industry and military computer systems has proceeded beyond the hacker stage to potentially hostile groups that have the means and expertise to wage offensive information warfare. The director of the U.S. National Security Agency(NSA), USAF Lt. Gen. Kenneth A. Minihan, stated, "This technology has become one of our most important sources of competitive advantage-and one of our greatest strategic vulnerabilities. Our ability to network has far outpaced our ability to protect ourselves from cyber attack."[4] We cannot avoid the issue at hand posed by these new electronic capabilities. The United States military and the Department of Defense are faced with the sobering thought that a ruthless low-tech enemy could exploit our vulnerabilities by using these new technologies to humble even the high and mighty United States of America. Government and industry must work together to make sure that the threat is manageable. It is a sharing of risks that must be undertaken to resolve this problem. Are we prepared for Cyber War? The underlying theme is that the United States still has no coordinated and comprehensive plan for addressing security concerns or for developing an overall national strategy.[5]

DISCUSSION

Information warfare and operations is here to stay. Former Secretary of Defense William Perry stated, "We live in an age that is driven by information. Technological breakthroughs are changing the face of war and how we prepare for war."[6] The usefulness of these information systems and the increasing access to information also make it vulnerable. These susceptibilities are a two edged sword--one side being the capabilities the Defense Department must protect and the other being capabilities that can be used against our adversaries.[7] Because of these problems, information by itself is becoming important to national security.

American officials and business leaders are becoming increasingly concerned about United States' liability to information warfare attacks on the nation's computers and electronic data networks by weekend hackers, terrorists, or enemies. Apprehension is growing as the nation's military, financial, business and government sectors become more interlinked and dependent on expanding worldwide communications networks.[8] As Anne Wells Branscomb has pointed out, "In virtually all societies, control of and access to information became instruments of power so much so that information came to be bought, sold, and bartered by those who recognized its value."[9] Martin C. Libicki of the National Defense University has stated that "hacker attacks on commercial information systems can distract the political leadership from national security duties."[10] The government is coming to the full realization that action must be taken to secure the nation's critical infrastructures from electronic attacks. The government slowly began to ramp up its efforts to ward off the potential catastrophic effects of information operations.

The President's Commission on Critical Infrastructure Protection was appointed by President Clinton in July 1996 to examine the vulnerabilities of the nation's core infrastructures. The Commission identified the following problems which resulted from the growth and progression of Information Technology:

> Our national defense, economic prosperity, and quality of life have long depended on the essential services that underpin our society. These critical infrastructures--energy, banking and finance, transportation, vital human services, and telecommunications--must be viewed in a new context in the information Age. The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence. This interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk.[11]

Shortly thereafter the National Defense Panel was asked to look at some of the long-term issues facing U.S. defense and national security. The panel reported to Secretary of Defense William S. Cohen in December 1997 on the changes needed to ensure U.S. leadership and the security and prosperity of the American people in the 21st century. In the area of Information Operations they reported the following:

> The importance of maintaining America's lead in information systems--commercial and military--cannot be overstated. Our nation's economy will depend on a secure and assured information infrastructure. Given the importance of information--in the conduct of warfare and as a central force in every aspect of society--the competition to secure an information advantage will be a high-stakes contest, one that will directly affect the continued preeminence of U.S. power.[12]

There are many examples regarding risks for our nation in Information Operations. For instance, in 1995, Vladimir Levin, a 28-year old Russian biochemistry graduate student in St. Petersburg, using computer codes, broke into New York Citicorp's cash management computer. Before he finished he transferred more than $12 million to other banks and had access to the $500 billion daily transfer account.[13] By the time it was all over, it showed that an attack on any defense structure or economy could be initiated without warning, is extremely difficult to trace, and is sometimes unobserved.

The threat is no longer hypothetical. The tools are widely available on the Internet to anyone with a computer and a modem. The General Accounting Office recently estimated that Pentagon computers experience some 250,000 hacker attacks per year and that 65 percent of these attacks are partially successful.[14] The basic problem is that we cannot tell if the attacks are recreational, malicious or a full blown attack to topple the nation.

The United States uses nearly 50 percent of the world's computer capability and contains around 60 percent of the Internet assets. This nation is one of the most advanced and, most dependent users of information technology.[15] Table 1 shows the global technology trends and identifies how the knowledge and capability of those able to disrupt infrastructure networks is growing.

	in 1982	in 1996	in 2002
Personal computers	thousands	400 million	500 million
Local area networks	thousands	1.3 million	2.5 million
Wide area networks	hundreds	thousands	tens of thousands
Viruses	some	thousands	tens of thousands
Internet devices accessing the World Wide Web	none	32 million	300 million
Population with skills for a cyber attack	thousands	17 million	19 million
Telecommunication systems control software specialists	few	1.1 million	1.3 million

Table 1 - Global Technology Trends[16]

A recent Washington Times article tells of computer hackers being able to disable the military. It is based on the results of a military exercise called "Eligible Receiver." A team from the National Security Agency, using software tools obtained from "hacker sites" on the Internet, attacked the U.S. Pacific

Command, using global Cyberspace. Over a two week period the team found that they could have denied the Command's theater command and control capability, virtually undetected. The Pentagon found it to be "an important and revealing exercise that taught us we must be better organized to deal with potential attacks against our computer systems and information infrastructure."[17] This exercise shocked many in the Pentagon because of the relative ease in which such an attack could be accomplished.

Current national security policy and strategy for Information Operations has been slow in its development and is outlined in the following documents. The President's 1997 National Security Strategy states:

> The national security posture of the United States is increasingly dependent on our information infrastructures. These infrastructures are highly interdependent and are increasingly vulnerable to tampering and exploitation. Concepts and technologies are being developed and employed to protect and defend against these vulnerabilities; we must fully implement them to ensure the future security of not only our national information infrastructures, but our nation as well.[18]

Also, the joint warfighting community has moved quickly to include Information Warfare in joint operations. The Joint Staff, in cooperation with the Services, combatant commands and Defense Agencies is working toward implementing a common vision. These ideas are prominent in the Chairman JCS' roadmap--Joint

Vision 2010, which prepares the Armed Forces for the challenges of the 21st century. Joint Vision 2010 states:

> We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting, or denying an adversary's ability to do the same. There should be no misunderstanding that our effort to achieve and maintain information superiority will also invite resourceful enemy attacks on our information systems. Defensive information warfare to protect our ability to conduct information operations will be one of our biggest challenges in the period ahead.[19]

The joint warfighting community sees the compelling need and its relevance to the Warfighter and is acting to raise awareness on Information Warfare within the Department of Defense. This is extremely important as the large force structures of the past transition to tomorrow's smaller, higher trained, and technically equipped forces. Additionally, the Quadrennial Defense Review (QDR) report prepared by the Secretary of Defense states that "although our current capabilities are adequate to defend against existing information operations threats, the increasing availability and decreasing costs of sophisticated technology to potential adversaries demand a robust commitment to improve our ability to operate in the face of information threats as we approach the 21st century."[20] While all of these policy documents are fine and can be used for the separate agencies there is no single agency within the government that can pull all these activities together.

RECOMMENDATIONS

There is no shortage of interest and concern, especially in the government arena and the Defense Department, regarding Information Warfare. The Office of the Secretary of Defense recently had RAND research this area. RAND is a nonprofit institution that helps improve public policy through research and analysis. Their recent report "Preparing for Conflict in the Information Age" identified the following:

> At present, the U.S. military is the world's leader in thinking, planning, and preparing for the advent of cyber war, both offensively and defensively. The United States is the only country with an array of advanced technologies as well as the organizational and doctrinal flexibility to make cyber war an attractive and feasible option. But its potential adversaries especially nonstate adversaries, may have lead in regard to a comprehensive information-oriented approach to social conflict. Here, the U.S. emphasis may have to be on defensive measures.[21]

Additionally, there is no apparent focus as current efforts appear specialized and non-complementary.[22] As a result, the Clinton Administration is currently trying to concentrate more attention on the problem. In July 1996, President Clinton created the Commission on Critical Infrastructure Protection and charged it with examining vulnerabilities in broad commercial systems, including telecommunications networks.[23] The executive order creating the commission identified that, "certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[24] This joint private sector and government commission were created to develop a national strategy for protecting the country's critical infrastructures from a spectrum of threats and to assure their continued operation. The chairman of the President's Commission, retired USAF General Robert T. Marsh, commented that "our security, economy, way of life, and perhaps even survival are now dependent on the interrelated trio of electrical energy, communications, and computers."[25] The group identified eight critical infrastructures to include the electric power system, gas and oil storage and transportation, water supply systems, telecommunications, banking and finance, transportation, emergency services, and continuity of government services. The Commission had this to say:

> Our national defense, economic prosperity, and quality of life have long depended on the essential services that underpin our society. These critical infrastructures must be viewed in a new context in the Information Age. The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence. This interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk.[26]

In the spirit of being able to shape, respond, and prepare now, in an integrated strategic approach, the Secretary of Defense outlined in the QDR that: "Defense against hostile information operations will require unprecedented cooperation between the Department of Defense, other federal agencies, the armed forces, commercial enterprises, our allies, and the public. The Department is working closely with the Presidential Commission on Critical Infrastructure to develop this cooperative relationship."[27]

Not everyone believes the Pentagon or the nation is taking the problem Information Warfare presents seriously enough or allocating adequate resources for this effort.[28] According to a February 1997, Defense Science Board Task Force on Information Warfare defense, there is a need for "extraordinary" action to deal with the present and emerging attacks to information systems.[29] The panel warned of a potential national security disaster if certain remedial actions are not taken immediately. Currently the Pentagon is spending less than $1 billion per year on Information Warfare. The Task Force suggested the Pentagon seek an additional $3 billion over the next five years principally for defensive measures. Finally, the three following recommendations were proposed: create an accountable Information War chief, establish minimum information protections across all of the armed services, and resolve legal and jurisdictional issues.[30]

In June 1996, then CIA Director John Deutch identified Cyberspace attack as one of the top threats to national security. He ranked it third behind proliferation of weapons of mass destruction and the potential of terrorist use of them. In his words, the U.S. is "not well organized as a government to address" the Cyberspace threat.[31] He claims that the increasing potential of Information Warfare endangers the disruption of everything electronic in the United States from air traffic control system and banking networks to power plants and military installations. Director Deutch named three priorities to improve our cyber warfare capabilities: create an Information Warfare Technology Center, chartered to serve both domestic and military security; improve tracking of threats posed by national and subnational groups; and development of a "defense-in-depth" response which incorporates as many barriers as possible within networks to preclude penetration.[32]

Former Senator Sam Nunn warned that the threat is mounting because sophisticated computer viruses enable adversaries to launch untraceable attacks from anywhere in the world. He said, "We often can't tell if an attack is from a United States person or from a foreign state."[33]

When The President's Commission on Critical Infrastructure Protection released their report and briefed the President in October 1997 relatively little progress has been made since then in forming a national consensus on the issue of defending critical infrastructures against cyberterrorists and hackers. Since industry owns the infrastructure and not the government this will only work when the various parties are united against a common threat. There are many reasons for this reluctance. The Commission Chairman General Robert Marsh said:

> The single most important recommendation of the panel is to develop information sharing arrangements in the private sector and between government and industry in areas such as unauthorized intrusions. The biggest obstacle to implementing the group's recommendations is the cultural change we have to bring about.[34]

Some owners of the infrastructure, especially the financial institutions, find that it is more acceptable to permit an intrusion into their networks rather than make a public acknowledgment that they have been "hacked." To do so would admit that security has been breached and place doubt in the minds of the consumer. The industry would make itself liable if it acknowledges a difficulty. The problem is reduced to becoming a write-off or cost of doing business in the information age.

The Federal Bureau of Investigation(FBI) has recently formed the National Infrastructure Protection Center. This organization is principally geared toward emphasizing the potential threats from electronic attacks to the private sector owners and operators of the infrastructure.[35] Currently the biggest drawback is the legal impediments to sharing the vast amounts of information that is needed to be shared with the operators of these critical infrastructures. The FBI is finding a need to switch from a criminal surveillance approach to one of exploiting intelligence surveillance. This is just one of several organizations that have recently been created to meet the new requirements of Cyberspace defense.

Another group, the Information Operations Technology Center was formed in August 1997 to help guard against computer network attack. It is a joint initiative of the Department of Defense and the Intelligence Community. It was formed to develop and apply telecommunications and computer technologies to Information Operations national security problems.

The Department of Defense is currently trying to get its act together with the development of a joint task force to control both offensive and defensive strategic and tactical Information Operations. It is still in the formative stages and somewhat disjointed per Deputy Secretary of Defense John Hamre. Mr Hamre said that although DoD is still working to determine "the focal point for [network] protection and Information Operations," the Pentagon will eventually create a joint task force to handle Information Operations.[36] The new task force most likely will be located in one of the DoD's Unified Commands such as the Atlantic Command, The Special Operations Command, the European Command or the Pacific Command. Furthermore, the Department of Defense is also looking at overall network security becoming the responsibility of the Defense Information Systems Agency.

The Joint Chiefs of Staff established the philosophy of a teamed approach being essential to developing a comprehensive

Information Warfare strategy. The Joint Staff brochure on Information Warfare outlines this policy with the following:

> We must assist in demonstrating to service providers the compelling need for a collaborative, teamed approach in crafting solutions-not just to support the Department of Defense and to protect our national security, but to protect their own proprietary interests as well.[37]

Being able to provide capabilities to support military operations require assured infrastructure beyond the peacetime information environment. This is necessary for mission success. However, one quickly realizes that the authority for protection implementation is outside the government and the Department of Defense. This is where all these new organizations still fall short is having a significant involvement by the industry members who own and operate the infrastructure. Robert Steele gives a rather scathing account that echoes this sentiment in his article, "Takedown: Targets, Tools, & Technocracy" with the following:

> The President's Commission on Critical Infrastructure Protection was at once a small sign of hope and a large symbol of despair. Apart from the fact that it did not talk to any of the serious professionals outside the beltway, and even more so, outside the nation, who actually know in detail the vulnerabilities and solutions the Commission was supposed to address...unfortunately, it did not give the Nation what it needed, and we are left--with no clear cut direction, no one clearly in charge, and no basis for which to mobilize the private sector into its new and urgent role as the first line of national defense against cyber-attack and self-destructive electronic systems.[38]

These recent incidents have been serving as a wake-up call for the military and the federal government that the idea of a cyber attack no longer seems remote. More attention to Information Technology security is what is needed. Doctrine and policy have not caught up with technology to combat the threat. To ensure this is accomplished more resources and high-level management attention is required. A national policy would focus that attention. It would provide a framework for government and industry to manage the synergistic effect of reducing risk across the infrastructures. Industry is still not trustful of government security. The key is how to get the intelligence community and the military to share the information once it is obtained. A focused national security policy would break down many of the barriers that impede successful implementation of combating this threat.

CONCLUSION

High-tech Information Warfare is fast becoming a reality. Rapid technological change presents a new challenge for strategists mastering the emerging forms and functions of information technologies.[39] The very nature of this technology makes us vulnerable. Recent events have continued to enforce the need for some sort of protection. Meeting the challenge today means understanding the implications of warfare in the information age. As nation-states become more adept in exploiting this technology our concern must increase because a much higher level threat exists that has the resources and ability to cripple the life support systems of our nation. This challenge requires the expansion and rapid acquisition of technology that includes the integration of global information systems.[40] It must be a collaborative effort. There is a changing balance of information control. In the information infrastructure arena, the government first had the lead; now industry does. Today the commercial sector is advancing computer and communications technologies at an extremely rapid pace. Military requirements no longer dictate the direction and speed of technology, forcing reliance on commercially available hardware and software.[41] The military services need to see what they can offer and leverage the commercial sector to put in the security that is needed. When the government controlled the infrastructures it was far easier to take a risk avoidance approach or posture. It is not possible to have risk free information systems or telecommunications environment therefore the risks must be managed. Mr Frederick G. Tompkins, former director of policy analysis for the National Computer Security Association, states that "a systems approach to information security management must be taken and there is no 'silver bullet' to resolve the many issues associated with the security of the digital world. A certification and testing program must be undertaken to make the risks manageable."[42] It is not possible to have risk free information systems or telecommunications environment. One cannot avoid risks as the very nature of technology makes us vulnerable. Therefore the risks must be managed.

Defensive Information Warfare has to be considered and integrated at all levels of conflict and applied across the full spectrum of military operations. This mandates that defensive Information Warfare be organized as a system and linked together by policy, doctrine, and a national supporting organizational infrastructure.[43]

Although current direction is sound, we must take it to the next higher echelon by establishing a national information strategy. The importance of information dominance requires a top-down establishment of a national strategy. It must have focused leadership for end-to-end consideration of all the needed and integrated components of a most complex national scheme.[44]

It is time to develop and implement a national level information strategy to tie together any fragmented capabilities in the Information Warfare arena in the private sector, the government, and the military.[45] We must integrate into national security strategy a strategic focus incorporating all of our operational centers of gravity. Instead of a piecemeal approach we must take advantage of the synergism all players offer and provide a more economical way of reaching the objective of Information Warfare security.

ENDNOTES

[1] David H. Freedman and Charles C. Mann, At Large (New York, N.Y., Simon and Schuster, 1997), 19.

[2] John Arquilla and David Ronfeldt, In Athena's Camp (Washington, D.C.: National Defense Research Institute, 1997),6.

[3] John Arquilla and David Ronfeldt, "Networks Weave a New Web of Life," Los Angeles Times, 14 December 1997, sec. M, p.5.

[4] Craig Covault, "Cyber Threat Challenges Intelligence Capability," Aviation Week & Space Technology, 10 February 1997,20.

[5] Chris O'Malley, "Information Warriors of the 609th,"Popular Science, July 1997, 74.

[6] Roger C. Molander, "Strategic Information Warfare, A New Face of War," National Defense Research Institute, 1996, xi.

[7] John M. Shalikasvili, "A Strategy for Peace..The Decisive Edge in War," Information Warfare, December 1996, 1.

[8] Jonathan S. Landay, "US Worries About Growing Threat of "Cyberwar" in Information Age," Christian Science Monitor, 7 June 1996, 1.

[9] Martin C. Libicki, What is Information Warfare?, (Washington, DC, National Strategic Studies, 1996), 7.

[10] Ibid.,58.

[11] The President's Commission on Critical Infrastructure Protection, Critical Foundations Protecting America's Infrastructures, (Washington, D.C., October 1997),35.

[12] The National Defense Panel Report, Transforming Defense--National Security in the 21st Century, (Washington, D.C., December 1997), 13.

[13] Timothy L. Thomas, "Deterring Information Warfare: A New Strategic Challenge," Parameters: Journal of the US Army War College, Winter 1996-1997, 81.

[14] Peter Grier, "At War with Sweepers, Sniffers, Trapdoors, and Worms," Air Force Magazine, March 1997, 23.

[15] John Correll, " War in Cyberspace," Air Force Magazine, January 1998, 35.

[16] Ibid.

[17] Bill Gertz, "Computer hackers could disable military," Washington Times, 16 April 1998, sec. 1A, p. 1.

[18] The White House, "A National Security Strategy for a New Century," National Security Strategy of the United States, May 1997, 14.

[19] Chairman of the Joint Chiefs of Staff, "America's Military: Preparing for Tomorrow," Joint Vision 2010, 16.

[20] William S. Cohen, Secretary of Defense, Report of the Quadrennial Defense Review, May 1997, 50.

[21] John Arquilla and David Ronfeldt, In Athena's Camp, 7.

[22] William B. Scott, "Information Warfare Policies Called Critical to National Security," Aviation Week & Space Technology, 28 October 1996, 60.

[23] Grier, 24.

[24] John Schwartz, "Retired General's Mission: Making Cyberspace Secure," Washington Post, 31 January 1997, p.19., col 1.

[25] Correll, 34.

[26] President's Commission on Critical Infrastructure Protection, ix.

[27] Cohen, 50.

[28] Grier, 24.

[29] Gerald Green, "DSB Warns US in Jeopardy from Information Warfare Threat," Journal of Electronic Defense, February 1997, 15.

[30] O'Malley, 74.

[31] Paul Mann, "Cyber Threat Expands With Unchecked Speed," Aviation Week & Space Technology, 8 July 1996, 63.

[32] Mann, 64.

[33] Mann, 63.

[34] Charlotte Adams, "Commission Urges Cooperation Between Government, Industry," 20 October 1997; available from <http://www.fcw.com/archive/1997/Q4/fcw-commission-10-20-1997.html>; Internet; accessed 29 April 1998.

[35] Heather Herreld, "Groups Join to Protect Critical Information Technology," 15 September 1997; available from <http://www.fcw.com/archive/1997/Q3/fcw-polsecur-9-15-97.htm>; Internet; accessed 29 April 1998.

[36] Bob Brewin, "Hamre Foresees Joint Task Force for Info Ops at DoD," 23 April 1998; available from <http://www.fcw.com/pubs/fcw/1998/0420/web-hamre-4-23-1998.html>; Internet; accessed 29 April 1998.

[37] Shalikashvili, 4.

[38] Robert D. Steele, "Takedown: Targets, Tools, & Technocracy," Manuscript prepared for U.S. Army War College Ninth Annual Strategy Conference, 31 March - 2 April 1998. 3.

[39] Timothy L. Thomas, "Deterring Information Warfare: A New strategic Challenge, "Parameters: Journal of the US Army War College, Winter 1996-1997, 81.

[40] Clarence A. Robinson, Jr., "Information Warfare Demands Battlespace Visualization Grasp," Signal, February 1997, 20.

[41] Scott, 60.

[42] Frederick G. Tompkins, "The Effect of Certification on Information Security Risk Management," National Computer Security Association White Paper, 1997, 4.

[43] Shalikasvili, 7.

[44] Scott, 64.

[45] Robert D. Steele, "Smart Nations: Achieving National Security and National Competitiveness in the Age of Information," American Society for Information Science, October 1996, 10.

BIBLIOGRAPHY

Adams, Charlotte. "Commission Urges Cooperation Between Government, Industry," 20 October 1997; available from <http://www.fcw.com/archive/1997/Q4/fcw-commission-10-20-1997.html>. Internet. Accessed 29 April 1998.

Arquilla, John and David Ronfeldt. In Athena's Camp Washington, D.C.: National Defense Research Institute, 1997.

________."Networks Weave a New Web of Life," Los Angeles Times, 14 December 1997, sec. M, p.5.

Brewin, Bob. "Hamre Foresees Joint Task Force for Info Ops at DoD." 23 April 1998. Available from <http://www.fcw.com/pubs/fcw/1998/0420/web-hamre-423-1998.html>. Internet. Accessed 29 April 1998.

Chairman of the Joint Chiefs of Staff, "America's Military: Preparing for Tomorrow." Joint Vision 2010, 1-34.

Cohen, William S., Secretary of Defense, Report of the Quadrennial Defense Review. May 1997, 50.

Correll, John. " War in Cyberspace," Air Force Magazine. January 1998, 33-36.

Covault, Craig. "Cyber Threat Challenges Intelligence Capability." Aviation Week & Space Technology. 10 February 1997, 20-21.

Freedman, David H., and Charles C. Mann, At Large. New York, N.Y., Simon and Schuster, 1997.

Gertz, Bill. "Computer hackers could disable military." Washington Times. 16 April 1998, sec. 1A, p. 1.

Green, Gerald, "DSB Warns US in Jeopardy from Information Warfare Threat," Journal of Electronic Defense. February 1997, 15.

Grier, Peter, "At War with Sweepers, Sniffers, Trapdoors, and Worms," Air Force Magazine. March 1997, 20-24.

Herreld, Heather. "Groups Join to Protect Critical Information Technology." 15 September 19997. Available from <http:;//www.fcw.com/archive/1997/Q3/fcw-polsecur-9-15-97.htm>. Internet. Accessed 29 April 1998.

Landay, Jonathan S., "US Worries About Growing Threat of "Cyberwar" in Information Age, Christian Science Monitor, 7 June 1996, 1.

Libicki, Martin C., What is Information Warfare?. Washington, D.C., National Strategic Studies, 1996.

Mann, Paul "Cyber Threat Expands With Unchecked Speed," Aviation Week & Space Technology, 8 July 1996, 63-64.

National Defense Panel Report, Transforming Defense--National Security in the 21st Century, (Washington, D.C., December 1997), 13.

O'Malley, Chris, "Information Warriors of the 609th,"Popular Science, July 1997, 74.

President's Commission on Critical Infrastructure Protection, Critical Foundations Protecting America's Infrastructures, (Washington, D.C., October 1997), ix.

Robinson, Clarence A., Jr., "Information Warfare Demands Battlespace Visualization Grasp," Signal, February 1997, 17-20.

Schwartz, John, "Retired General's Mission: Making Cyberspace Secure," Washington Post, 31 January 1997, p.19., col 1

Scott, William B., "Information Warfare Policies Called Critical to National Security," Aviation Week & Space Technology, 28 October 1996, 60-64.

Steele, Robert D., "Smart Nations: Achieving National Security and National Competitiveness in the Age of Information," American Society for Information Science, October 1996, 10.

________."Takedown: Targets, Tools, & Technocracy." Manuscript prepared for U.S. Army War College Ninth Annual Strategy Conference. 31 March - 2 April 1998. 3.

The White House, "A National Security Strategy for a New Century," National Security Strategy of the United States, May 1997, 1-29.

Thomas, Timothy L., "Deterring Information Warfare: A New Strategic Challenge." Parameters: Journal of the US Army War College, Winter 1996-1997, 81-91.

Tompkins, Frederick G. "The Effect of Certification on Information Security Risk Management." National Computer Security Association White Paper, 1997, 4.

DOCUMENT 2

Cyber-Terrorism: Modem Mayhem

AD-A345705

1998

U.S. Army War College
Carlisle Barracks, Pennsylvania

STRATEGY RESEARCH PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

CYBER-TERRORISM: MODEM MAYHEM

BY

COLONEL KENNETH C. WHITE
United States Army

USAWC CLASS OF 1998

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

Cyber-Terrorism: Modem Mayhem

by

COL Kenneth C. White

Robert D. Johnson
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: **Kenneth C. White (COL), USA**

TITLE: **Cyber-Terrorism: Modem Mayhem**

FORMAT: **Strategy Research Project**

DATE: **14 April 1998** PAGES: **38** CLASSIFICATION: **Unclassified**

America can no longer rely on broad oceans and a strong military to protect its homefront. The arrival of the information age has created a new menace--cyber-terrorism. This threat recognizes no boundaries, requires minimal resources to mount an attack, and leaves no human footprint at ground zero.

This study addresses technology, identification procedures, and legal ambiguity as major issues, for countering cyber-terrorism as an emerging challenge to U.S. national security. As America's reliance on computer technology increases, so does its vulnerability to cyber attacks.

TABLE OF CONTENTS

> U.S. vulnerability to [cyber-terrorism is] the major security challenge of this decade and possibly the next century.[1]
>
> — Joint Security Commission

For more than 200 years, America's homeland has enjoyed protection from attacks because of broad surrounding oceans and a strong military force. However, the arrival of the information age[2] has dramatically changed America's defense posture: How can we protect our recently developed critical information infrastructure? According to the Presidential Commission on Critical Infrastructure Protection, "as networked computers expand their control over the nation's energy, power, water, finance, communications, and emergency systems, the possibility of electronic attack and catastrophic terrorism becomes increasingly possible."[3]

Yearly, commercial businesses and government organizations lose valuable data, time, and money because computer systems are compromised. Annually, some 250,000 attempts to penetrate U.S. Department of Defense (DoD) computer systems are recorded. Sixty-five percent of these attempts are successful.[4] For example, in February 1998, as the U.S. was stepping up deployments of troops and equipment to the Persian Gulf, 11 U.S. military computer systems were comprised--seven Air Force systems, four Navy systems. Those compromised contained logistical, administrative, and pay records data. Such intrusions potentially cause widespread confusion and disruption of military operations. They certainly call into question the integrity of security for our DoD computer systems. Investigating authorities have stated that recent breaches of military computers are the most organized and systematic attacks on U.S. defense networks to date. Sources of these attacks have not been identified.[5]

Other compromises of national critical infrastructure network components include an October 1997 compromise of the Pacific & Electric Company's network, which caused widespread power outages in San Francisco, California. Also switchboards in Florida were jammed intermittently for months in 1996, which prompted a global hunt for the attacker by the Federal Bureau of Investigations. Likewise, another high profile hacker (a person who attempts to penetrate security systems on remote computers as a challenge) intrusion occurred during the summer of 1995, when several military and university computer systems containing important and sensitive information about satellites, radiation and energy were compromised.[6] These cases involve hacker break-ins to computer systems, not cyber-terrorists attacks. However, hackers and cyber-terrorists differ only in their intentions: Hackers may be only criminally destructive adventurers, whereas cyber-terrorists are advanced enemies of a nation state.

"The information age promises an explosion in economic growth, technological innovation and educational opportunities that could improve the standard of living and quality of life around the world."[7] However, an unintended consequence of information age triumphs is the creation of a new problem--cyber-terrorism. Barry Collins, an analyst for the Institute for Security and Intelligence, coined the term "cyber-terrorism" a decade ago. He identifies cyber-terrorism as "the intentional abuse of a digital information system, network, or component toward an end that supports or facilitates a terrorist campaign or action."[8] Current corporate and government practices to computerize more and more tasks and processes plays into the hands of the cyber-terrorist.

Documented evidence indicates several terrorist organizations have incorporated information age technology into their terroristic strategies. For example, the Italian Red Brigade's manifesto specifies attacking computer systems as an objective for striking a state's center of gravity. Law enforcement and intelligence officials say various terrorist organizations operating in the U.S. are making full use of technology to link their World Wide Web sites, to solicit funds, to transfer funds to anonymous off-shore bank accounts, and to stage attacks.

John Deutch, then Central Intelligence Agency Director, in testimony before Congress in June of 1996, warned that "the ability to launch an attack on the U.S. infrastructure via computer-generated terrorism, the ultimate precision-guided weapon, is already in the hands of terrorist organizations".[9] Indeed, "modem mayhem[10]" is plausible.

This study addresses several issues that characterize cyber-terrorism as an emerging challenge to U.S. national security. The background establishes a frame of reference for understanding cyber-terrorism. Secondly, the challenges are analyzed in terms of major issues related to cyber-terrorism: technology, identification procedures, and legal ambiguity. This study concludes with recommendations for limiting vulnerabilities of critical U.S. infrastructure computer networks to cyber-terrorism.

BACKGROUND: Evolution in Revolution

> I am a computer revolutionary. If a revolutionary is a terrorist, then a computer revolutionary is a computer terrorist and therefore, I am a computer terrorist.[11]
>
> — Rop
> European Hacker

U.S. national security experts list terrorism as one of the top current menaces. However, terrorists have recently implemented new strategies utilizing information age tools. Given the minimal requirement of a personal computer, modem, telephone connection, and a few well placed key strokes to orchestrate an attack on a nation's electronic infrastructure, a new terrorist species has evolved, the cyber-terrorist. The cyber-terrorist practices cyber-terrorism, a new breed of terrorism.[12] Just as nations have exploited technology in their national interest, cyber-terrorists have also leveraged technology in pursuit of exploiting the power of information tools in their interests.

Historically, the form of terrorism dominant during the Cold War was ideological terrorism, and could be categorized as either Marxist or nationalist. For example, the Italian-based Marxist Red Brigade, very active in the 1980s, seeks to create his own revolutionary state through armed struggle and to separate Italy from the Western Alliance. This group concentrated on assassination and kidnapping of Italian government officials and influential, private sector leaders. However, Americans were also targeted. U.S. Army Brigadier General James Dozier was kidnapped in 1981 and Leamon Hunt, U.S. Chief of the Sinai Multinational Force and Observer Group, was murdered in 1984 by the Red Brigade to protest U.S. and NATO forces presence in Italy, as well as their foreign policies.[13]

In the wake of the Cold War, ethno-religious and single-issue terrorism was most prevalent. Ethno-religious terrorism was responsible for the 1993 World Trade Center bombing in New York City by militant Islamic radicals who view the U.S. as the "Great Satan", an enemy of Islam that must be punished. The 1995 bombing of Oklahoma City's Alfred P. Murrah Federal Building was an example of single-issue terrorism. Prosecutors contend that the conspirators responsible for the bombing sought retaliation for the federal government's 1993 siege of and attack on the Branch Davidian compound at Waco, Texas. Some terrorist experts, supported by their research, contend that single-issue terrorism has the potential to be the most prevalent terrorism form to occur domestically.

Some of the organizations, groups, and individuals who have shown an inclination to implement single-issue terrorism include radical environmentalists, pro-life movement extremists, animal rights extremists, separatist groups, millenium watchers, cultists, survivalists, neo-fascists, drug and other criminal cartels, as well as disgruntled employees. Representatives of all these groups reside and are active in the U.S.

Who or what do these terrorist groups target? The President's Commission on Critical Infrastructure Protection has identified eight critical U.S. infrastructures at risk: telecommunications; transportation (aviation, shipping, trucking and rail industries); electrical power systems; water supply systems; gas and oil storage and transportation; emergency services; banking and finance; and continuity of government services.[14] Not all of these systems are networked, but all are becoming so. Even systems in a "stand alone" mode are vulnerable to several kinds of attacks. One vulnerability can be exploited through a modem and social engineering. The terrorist pose as a new employee in need of assistance to access company computers in order to acquire data on internal security, passwords, and system configurations. Similarly, "Trusted Insiders" use their direct access to destroy or manipulate the data or computer networks from within. Sometimes they insert a malicious code during outside service calls, contractor network upgrades, or through loading unsolicited software. Even software received anonymously in the mail may carry out such insidious disruption; it may indeed be innocently introduced to a targeted system.

What objectives cyber-terrorists achieve through such relatively easy intrusions? The cyber-terrorist has three potential objectives: destruction, alteration, or acquisition and retransmission of data/commands. Achievement of any of these objectives could have a potentially devastating impact on the intended target.

What are cyber-terrorists' weapons? Weapons of choice are electronic in nature. They require only time to create a list of instructions for the computer to follow and a few key strokes to deliver those instructions. Computer viruses are the oldest and best-known software weapons. They invade computer systems and reproduce themselves, destroying data and/or hardware. Most viruses use the hitchhiker approach to enter a computer system. Like biological viruses, the computer virus is silent and invisible; it does not show itself until the targeted system is already infected.[15]

Another weapon is the worm. "Worms are breeder programs, reproducing themselves endlessly to fill up memory and hard disks. Worms are often designed to send themselves throughout a network, making their spread active and deliberate."[16]

A third weapon is the logic bomb, which is difficult to locate. The logic bomb is a set of destructive instructions that detonate on a predetermined date. It may also detonate when a specific set of instructions is executed, causing damage within the computer or throughout a network.

Bots are a fourth weapon of the cyber-terrorist. The bot is derived from robot; it is code-designed to recon the Internet and carry out designated tasks. For instance, it may retrieve or destroy specified data. The SYN attack is a similar bot weapon. It floods a host server and causes a bottle-neck or traffic jam. Server access slows to a crawl or is disabled.

Finally, extortion can be used just as effectively as one of the weapons listed above. Recent reports indicate that banks have paid hackers upwards to six figures to prevent them from using the banks' compromised security codes. Also, in the past year, corporations have lost in excess of $800 million as a result of computer break-ins.[17]

The above list of cyber-terrorist weapons is by no means exhaustive. It is merely a representative sampling of tools in the hands of John Q. Cyber-Terrorist. A radical European computer hacker proclaimed, "You see, computers are to be used as a tool for the revolution. It is up to us to stir up the social system. It's not working. We have to make the waves."[18] As America's dependence on computers continues to flourish, John Q. Cyber-Terrorist no doubt looks at the U.S. as a target rich environment. His new maxim may be, "So many new targets...so little time".[19]

CHALLENGES: TECHNOLOGY

> In the future, factories will have only two employees, a man and a dog. The man to feed the dog and the dog to keep the man away from the computers.[20]
>
> — Anonymous

Technology enables cyber-terrorists to maintain anonymity. "No airport checkpoints to pass through. No fingerprints left on the steering wheels or bomb fragments. No human presence at ground zero."[21]

Since information system knowledge doubles every twelve months and since this growth continues to accelerate, security procedures cannot keep pace with technology improvements. By the time the full impact or significance of a technological improvement is known, new advancements are already on the market.[22] As technology becomes more cost effective, cyber-terrorists become more technologically oriented in their tactics and strategies.

Technology has linked America's critical infrastructure systems together so tightly that an attack on any link could very well have cascading impacts, eventually affecting several or all systems. Unfortunately, the U.S. is the leading, worldwide consumer of digitization; the nation has become enthralled with the plethora of data available at the users' fingertips. Americans expect their computers to work all the time, exactly when they want them to. If such expectations are not fulfilled, this dependence forces a virtual productivity shutdown.

Sophisticated cyber-terrorists recognize that a disruption of America's computer network will have cascading negative impacts. Frequent disruptions will initiate the desired effects of fear, panic, and a loss of confidence in the nation's leadership to prevent future disruptions. Imagine the havoc created if only a region of America's financial network was successfully attacked: No stock or credit card transactions, personal and corporate banking accounts deleted, and automatic telemachines being rendered inoperative. No doubt, mass hysteria would result. The most frightening aspect of the above scenario is that the tools and techniques for creating such havoc are readily available today. A few select commands to key power grids could cause a massive power outage for days, possibly for weeks--especially if the main computer, as well as the backup software, were corrupted as a result of a cyber attack.

Technological advances in hardware, software, and the Internet are enabling private citizens, businesses, government, and DoD to obtain sensitive data for legitimate purposes. But these advancements also assist cyber-terrorists in the conduct of illegitimate activities.[23] A cyber-terrorist's primary tools are the personal computer (PC), the modem, and a telecommunications line. Approximately every twelve months, the PC is enhanced by increased processing speed, increased CD ROM speed, increased data storage capacity, improved reliability, improved mobility, and greater acceptance because of lower prices and ease of operation.

The second hardware tool is the modem. It is also enhanced on an ongoing basis to increase data transmission speed and reliability. These enhancements likewise enable the cyber-terrorist to transmit his destructive commands faster and more accurately.

The cyber-terrorist also has easy access to the telecommunication line. Recent improvements have removed old wiring, which carried only one call per strand. It has been replaced by fiber optic cable, which can carry thousands of communication exchanges on one line smaller than a human hair. The fiber optic cable facilitates telecommunications transmission of video, data, voice, word, and images which can be transmitted one at a time or simultaneously. Fiber optic cable also easily encrypts data for security purposes.[24] Although legitimate users enjoy the many advantages of fiber optic cable use, the same advantages also enhance the cyber-terrorist's capability to attack and disrupt systems.

With one or more of these accessible tools of terror, the cyber-terrorist is almost ready to launch an attack. All he lacks is a set of programming instructions, the software. Some of the hacker software programs now available are SATAN, an infiltration program designed to automatically scan networks for documented security holes; PC Track, a program that tracks satellites orbiting the earth; and Virus Creation Lab, a combination of software codes that may be mixed and matched to create malicious virus programs.[25] Using this software, the cyber-terrorist, assisted by the PC, modem, and a telecommunications line, can rapidly access, destroy, alter, copy, or retransmit selected data.

He can also use the software advancement in cryptography, which is the science of code making and code breaking. Cryptography is no longer used primarily by the diplomatic and military establishments. Law-abiding private citizens, businesses, and government organizations are employing cryptography software to share information securely. Once again, cyber-terrorists now utilize cryptography software to carry-on illegal activities such as encrypting their message traffic from the prying eyes of law-enforcement agencies.[26]

Last but not least is the cyber-terrorist's ready access to the Internet. Some technical writers have proclaimed the Internet as the foundation for planetary connection and the ultimate pathway to democracy. However, like many powerful tools, the Internet can be abused. "The Internet, which was created in 1969 as a network for the U.S. Department of Defense, essentially is a network of networks (a large group of computers interlinked and capable of sharing information)."[27] The exponential growth of the Internet is based on its service to commercial activities. Business uses of the Internet range from internal and external communications to advertising and selling products.[28]

Americans are increasingly using the Internet, both for business, and for recreational and educational purposes. The Internet has far transcended its original purpose of enabling scientists to share information and resources with their colleagues across long distances and to provide an assured means of communicating with selected governmental proponents in the event of a nuclear war.[29] Today it provides multiple points of entry into computer systems connected to it. As the Internet grows, so do vulnerabilities, because computer systems linked through the Internet are less and less physically isolated and controlled. Instead, connections are more indiscriminate, access is less monitored and controlled. The Internet today consists of layers of systems distributed across many other systems which utilize network and application software too complex for a single individual to understand completely.[30]

In summary, technology employed by cyber-terrorists is readily available and cost effective. Access to it requires no state sponsorship. Technology provides a comfortable degree of anonymity and offers a multitude of points of entry to attack America's critical infrastructure systems remotely. Misuse of technology will continue to place America's critical networks at risk because of the constant improvements in technological capabilities and the cyber-terrorist's ability to quickly and relatively easily exploit these improvements.

IDENTIFICATION

Emerging technology has undoubtedly enhanced the cyber-terrorist's weapons arsenal. To compound the problem of countering cyber-terrorists, this technology has also diminished capabilities to identify perpetrators. As hardware (computers and modems) continues to shrink, cyber-terrorists' mobility increases. As the hardware's processing speed increases, the cyber-terrorists' on-line time to issue destructive commands or to communicate with compatriots likewise decreases, limiting defenders' chances of "catching them red-handed". As hardware prices fall, cyber-terrorists are ensured of ready access to state-of-the-art equipment. And as software enhancements are implemented, the cyber-terrorist's efficiency likewise increases. All told, computer systems security managers face a Herculean challenge to identify, with certainty, the cyber-terrorist.

Another technological innovation that hampers the identification of cyber-terrorists is the anonymous server. It sends message traffic through several electronic remailers. As the intruder's destructive signals traverse several anonymous servers located in far-flung parts of the world, their true origin is almost certainly masked.[31]

Likewise, the identification of state sponsored cyber-terrorism is definitely not a cut-and-dried proposition. The distinction between legitimate rational states and rogue states is blurred. "If a government could choose between perpetrating an attack through its own organs or contracting out, most would take the latter option quite seriously."[32] Why? Nations can always use the deniability screen provided by technology to proclaim their innocence. Even if the perpetrators are caught, identifying them as agents of a particular government is hardly guaranteed. Cyber-terrorists neither wear uniforms nor require special equipment available through sponsorship, such as tanks, planes, or submarines that may be traced.

Responding to a cyber-terrorist attack is a risky endeavor, especially if the attacker has not been positively identified. An offensive response triggering a retaliatory strike requires clear and positive identity of the attackers. But many questions must be answered prior to retaliation: How should the U.S. respond, through the use of military force, diplomatic channels, federal law enforcement, or a combination of the above? What are the criteria for responding? Depending on the nature and extent of the attack, should the response be through an alliance with a coalition of other nations or as a unilateral action? If such questions are not addressed, surely the situation could escalate beyond cyberspace, that virtual world where humans and computers co-exist, to a full scale conventional war.

Last but certainly not least in the identification arena is the owner-operators' inability to discern when a system is under attack. Only five percent of all victims know their networks are under attack. Of those who know of or suspect an attack, only two percent report it.[33] Unfortunately, owner-operators cannot distinguish an accidental outage or maintenance problem from a cyber-terrorist attack. The new breed of terrorists increasingly choose to remain anonymous after they have attacked, instead of identifying themselves as they have done in the past. The actual attack thus becomes an end unto itself according to several terrorism experts. Additionally, this lack of acknowledgement increases anxiety, tension, and uncertainty regarding follow-on attacks.

Given the low probability that a cyber-terrorist will be identified, thoroughly resourced attacks can be implemented at the time and place of the attackers' choosing. The President's Commission on Critical Infrastructure Protection concluded that cyber-terrorists are able to conceive, plan, and implement an attack with no detectable logistical preparations. "The target can be invisibly reconnoitered, the sequence of events clandestinely rehearsed, and an attack launched without revealing the identity of the intruder."[34]

AMBIGUITY

> Criminals [are] moving increasingly into cyberspace and without new laws, drug dealers, arms dealers, terrorists and spies will have immunity like no other.[35]
>
> — Louis Freeh
> FBI Director

In an era of global markets and global competition, the technologies to create, manipulate, manage, use, and protect critical infrastructure networks are of strategic importance to the U.S. However, the global information age challenges U.S. law and necessitates the creation of consistent multinational legal standards. How can the national security establishment better discern what is a politically motivated computer crime as opposed to a teenage computer prank? Criminal law has applied the so-called "rule of lenity" and imposed the burden of proof and persuasion on the prosecution. Thus, in order to impose criminal sanctions, laws protecting the informational infrastructure must clearly and unambiguously define which activities are permitted and which are proscribed.

Further, any doubts concerning the application of the law should be resolved in favor of the accused. If the law is too ambiguous to be assuredly applied or if it fails to define the nature of the proscribed conduct, the entire statutory scheme may be struck down as "void for vagueness."[36] The bottom line is that currently the prosecutor has the burden of proving beyond a reasonable doubt that the accused is guilty. Also, computer-related offenses without eyewitness testimony and physical evidence pose a major problem for law enforcement authorities. All too frequently, they cannot gather sufficient evidence to support a conviction of known culprits.

In fact, we have no generally accepted definition of what constitutes a computer crime, wherein terrorism has only a small part. Although the term "cyber-terrorism" was coined a decade ago, there is no indication that the State Department has adapted a useful definition of the term. The State Department's Anti-terrorism unit narrowly defines terrorism as only politically-motivated physical attacks. Thus computer network attacks generally do not conform to their definition of terrorism.[37] Ego-driven intrusions into a system to erase files or stealing information with the sole intent to blackmail is nothing more than simple theft, fraud, or extortion. Such intrusions do not constitute an attack on the government.[38] However, Ambassador Philip C. Wilcox, Jr., the State Department's coordinator for counter-terrorism, did address cyber-terrorism in his remarks to the 15th Annual Government/Industry Conference on Terrorism, Political Instability, and International Crime on 28 February 1997 in Washington, D.C.

Since cyber-terrorism respects neither national borders nor legal constraints, the challenge of international cooperation and coordination of investigations, coupled with diverse, overlapping and sometimes contradictory computer crime laws, regulations and criminal procedures, makes enforcement of criminal statutes even more difficult.[39] Understandably, sovereign nations are reluctant to release control over domestic issues or to allow foreign governments to impose laws on their citizens.

"It is commonplace to observe that states participate in international arrangements when it is in their best interest to do so, or when those arrangements can be molded to conform with states' perceived self-interests."[40] Governments around the world must acknowledge that their individual and collective self-interest lies in compatible legal procedures, workable international standards, and global cooperation.

Computer criminals are becoming increasingly sophisticated and knowledgeable. Some legal experts accordingly despair that cyberlaws (rules and regulations regarding behavior in the virtual computer world), like many other statutes "become obsolete as soon as they are passed with changes in behavior out stripping changes in the law."[41] Cyberlaw is currently only graduating from kindergarten. Lamentably, there is little consensus on how to proceed legislatively and judicially.[42]

A convincing argument can be made that it is in America's interest to take the lead in seeking global cooperation to establish compatible legal procedures and international standards. After all, America is the world's largest consumer of automation, even though it has only five percent of the world's population. The security of the nation's electronic infrastructure is too important for America not to seek more protective measures. Some defense and intelligence officials warn, that "as the United States becomes more dependent on computerized information systems, and links between these networks grow, so does the vulnerability to an electronic assault that could paralyze the country."[43]

DoD must assume a significant role in addressing cyber-terrorist attacks. But this emerging role, like laws governing computer crime, is currently ambiguous and uncertain. Of concern in some quarters is DoD's lack of authority to provide guidance on securing America's infrastructure networks, although the transmission of the majority of DoD's unclassified data utilizes public-switched networks. In view of DoD's broad mission to maintain the leading edge in warfighting capability and its current and historical role in the deployment and use of computers and computer networks, it is reasonable to assume DoD will be a key player during the formulation and implementation of a strategy to address cyber-terrorism. DoD possesses unique technical expertise, equipment, and experiences that are ideally suited to confront threats to America's critical computer networks.

Since cyber-terrorism knows no national boundaries and does not have to present a passport at borders, it will continue to flourish. Cyber-terrorists can ply their destructive trade far from the scene of the attack. Cyber-terrorists can stay at home and remotely perpetrate their misdeeds. Without cutting-edge standardized laws and international cooperation, cyber-terrorists remain mostly free to attack targets of their choice, when they choose. Until DoD's role in combating cyber-terrorism is defined, its potential assistance in defending critical infrastructure networks is limited.

RECOMMENDATIONS

> We should attend to our critical foundations before the storm arrives, not after: Waiting for disaster will prove as expensive as it is irresponsible.[44]
>
> — President's Commission on Critical Infrastructure Protection

Cyber-terrorism is constantly evolving. Effectively countering it requires adapting to a changing culture. Many procedures are available to challenge cyber-terrorism; however, network vulnerabilities cannot be eliminated through the use of any single procedure. In fact, all the holes will never be plugged because the challenge is dynamic and the cost of security is very high indeed. Although the federal government's budget for research and development of infrastructure protection is $250M annually, recommendations have been made to quadruple this figure over the next five years.[45] The following recommendations for public and private sector action are introduced as positive steps in limiting the cyber threat to America's critical infrastructure networks.

First, implement training programs in the public and private sectors to alert and inform users and operators of network vulnerabilities and procedures to reduce them. Prescribing a "PC lite" diet to America would not be an effective action plan. However, a widespread educational program to increase awareness of the problem holds considerable promise.

Second, we should leverage technology to limit computer network vulnerabilities. Such technologies as encryption, clipper chip,[46] and biometrics[47] are front runners in this area. Although the commercial sector does not endorse the clipper chip due to potential law enforcement monitoring of commercial dealings, such issues must be re-addressed so that necessary compromises lead to effective actions. The clipper chip encryption device should be designated as standard protection against network security breaches in both the commercial and government sectors. The degree of privacy that may be lost is miniscule compared to the degree of havoc that can be wreaked upon the nation's critical computer networks, to say nothing of the second and third order effects to follow. The U.S. should also take the lead in standardizing commercial encryption tools used internationally.

Third, rewrite and continuously update legislation to ensure it is unambiguous regarding what constitutes a computer crime. Agreements must be implemented to clarify legal proceedings within the U.S. and internationally. Laws, however, must be expansive enough to deter unlawful activities, but narrow enough to recognize the many legitimate uses of computers and computer networks.

Finally, we should create a coalition between private and public sector participants. Responsibility for the protection of the nation's critical computer networks crosses public and private sector boundaries. The coalition must clearly delineate the roles and missions of combatants of cyber-terrorism. From a military perspective, DoD's role in combating cyber-terrorism must be clearly specified to take full advantage of the unique skills and experiences that DoD possesses.

CONCLUSION

> Tomorrow's terrorists may be able to do more damage with a keyboard than with a bomb.[48]
>
> — National Research Council

In the past, America's homefront has been protected by large surrounding oceans and a strong military. However, the importance of those oceans and of military force has been decreased, thanks to wholesale acceptance of information age innovations. America's national security is currently challenged by a new menace, cyber-terrorism. Documented evidence, such as the Italian Red Brigade's manifesto, reveals that cyber-terrorism has been incorporated into some terrorists' campaign strategy. Unfortunately, the tools to orchestrate a computer-generated attack on critical U.S. infrastructure networks are readily available today.

Cyber-terrorists have leveraged technology to exploit the power of information age tools to the maximum extent possible. They have demonstrated their capabilities to use advanced technology, to travel and communicate undetected, and to circumvent the letter and spirit of the law. Computer networks that control the nation's critical infrastructure systems have already been infiltrated on many occasions, at many different sites.

Cyber-terrorism is dynamic. But its impact can be lessened through vigilance, cooperation, and a clear delineation of roles and missions for business, government, and DoD to combat cyber attacks. Although a devastating computer network attack has not yet occurred, known compromises of U.S. computer systems should serve as a warning sign of impending danger. As Senator Richard Lugar of Indiana observed, "People don't understand the enormity of the national security threats out there; we need to be vigilant. This is not a time to go to sleep at the switch."[49] Now is the time to establish procedures to address the emerging challenge of modem mayhem to national security.

Word Count=5,231

ENDNOTES

[1] Joint Security Commission, "Technology Report on Cyber-terrorism," 1994 p.1; available from: <http://www.mvhs.srusd.k12.ca.us/~kwade/techreport.html>; Internet; accessed 28 March 1998.

[2] Information Age - An era of a globally, computer interconnected society where information and economic value are nearly synonymous. Winn Schwartau. Information Warfare, (New York: Thunder's Mouth Press, 1996), 28.

[3] David Phinney, "Electronic Plan of Attack." 20 Oct 1997, p. 1. available from: <http://www.abcnews.aol.com/sections/us/cyberterror1020/index.html>; Internet; accessed 28 March 1998.

[4] Reid Kanaley, from the article "Analyst Finds U.S. Treasury, Military Computers Vulnerable to Infowar," available from: <wysiwyg://184/http://www.infowar.com/civil_de/civil_i.html-ssi>; Internet; accessed 27 March 1998.

[5] Bradley Graham, "11 U.S. Military Computer Systems Breached by Hackers This Month," 26 Feb 98, p. 1, available from: <http://www.infowar.com/hacker/hack_030498a_j.html-ssi>; Internet; accessed 16 November 1997.

[6] "Cyber Threats," available from: <http://www.infowar.com/hackers/hack.html>; Internet; accessed 26 March 1998.

[7] "Perspectives on Security in the Info Age," which outlines breaches of confidentiality, disruption of operations, and destruction of cyber property. Available from: <http://www.cspp.org/reports/report1-96.html>; Internet; accessed 16 November 1997.

[8] Matthew G. Devost, Brian K. Houghton, Neal A. Pollard, "Information Terrorism: Can You Trust Your Toaster,"available from: <http://www.terrorism.com/terrorism/itpaper.html>; Internet; accessed 16 November 1997.

[9] "New Security Threats Rest in Cyber Terrorism", 3 Feb 1997, available from: <http://www.infowar.com/civil_de/civil_c.html-ssi>; Internet; accessed 16 November 1997.

[10] Modem (Modulate - Demodulate): "A form of computer hardware that allows a computer to communicate with other computers…through telephone lines". Garry S. Howard, Introduction to Internet Security from Basics to Beyond, (Rocklin, CA: Prima Publishing, 1995), 354.

[11] Schwartau, p.357.

[12] Terrorism is "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." Douglas Platzer, "The Future of Terrorism," March 1997. Available from: <http://www.terrorism.com/terrorism>; Internet; accessed 29 November 1997.

[13] George Goncalves, "Terrorist Group Profiles: Red Brigade," Last Update, 2 Mar 97. Available from: <http://www.milnet.com/milnet/tgp/data/br.htm>; Internet; accessed 27 March 1998.

[14] Summary of the President's Commission on Critical Infrastructure Protection Survey conducted in 1996. The results will be used to "develop recommendations for research and development programs to address technology shortfalls and formulate critical infrastructure protection strategies." Available from: The Texas Transportation Institute's Information and Technology Exchange Center, <http://www.tti.tamu.edu/pccip>; Internet; accessed 29 November 1997.

[15] Schwartau, p. 156.

[16] "Net Apocalypse! - War: Cyber-terrorism," CNET, available from: <http://zeppo.cnet.com/Content/features/Dlife/apocalypse / ss02a.html>; Internet; accessed 12 February 1998.

[17] Ibid.

[18] Schwartau, p. 356.

[19] Sloan, p.4.

[20] Anonymous

[21] "Apocalypse Explained," CNET, 1997, available from: <http://zeppo.cnet.com/content/features/dlife/apocalypse/ss02a.html>; Internet; accessed 9 October 1997.

[22] James W. McLennan, "Battlefield of the Future." available from: <http://www.cdsar.af.mil/battle/chp7.html>; Internet; accessed 29 November 1997.

[23] Richard L. Field, "Electronic Banking: Banking Has Important Stake in Unfolding Cryptography Regulations." available from: <http://www.ctr.columbia.edu/vii/crypto/rlf2.htm>; Internet; accessed 29 November 1997.

[24] Kornel Terplan, Communication Networks Management, (Englewood Cliffs, NJ: Prentice Hall, 1992), 52.

[25] "Technology Report on Cyberterrorism," p.3, see endnote 1.

[26] Michael Alexander, Net Security: Your Digital Doberman (NC: Ventana Communications, 1997),73.

[27] Elizabeth Panska, PC Novice Guide to the Web, (Lincoln, NE: Peed Corporation, 1996),6.

[28] William Stallings, Internet Security Handbook, (Westport, CT: IDG Books Worldwide, 1995),185.

[29] Ibid.

[30] Kent Anderson, "Criminal threats to Business on the Internet," 23 Jun 97, p. 2; available from: <http://www.aranet.com/~kea/papers/white paper.shtml>; Internet; accessed 5 January 1998.

[31] Jean Guisnel, Cyberwars: Espionage on the Internet, (New York, NY: Plenum Trade, 1997), 132.

[32] Ibid., p.50.

[33] Ibid., p. 24.

[34] "The President's Commission on Critical Infrastructure Protection, Report Summary," Oct 97; available from: <http://www.pccip.gov/sumarry.html>; Internet; accessed 20 November 1997.

[35] REUTERS, "FBI Chief Calls for Computer Crime Crackdown," 28 Oct 97; available from: <wysiwyg://65/http://www.infowar.com/class_2103097b.html-ssi>; Internet; accessed 20 November 1997.

[36] Mark D Rasch, "Criminal Law and the Internet," in The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues, (The Computer Law Association, 1996), 1.

[37] Richard W. Aldrich, "The International Legal Implications of Information Warfare," Apr 96, available from: <http://www.usafa.af.mil/inss/ocp9.htm>; Internet; accessed 5 January 1998.

[38] Matthew G. Devost, Brian K. Houghton, Neal A. Pollard, "Information Terrorism: Political Violence in the Information Age," available from: <http://www.terrorism.com/denning.html>; Internet; accessed 11 January 1998.

[39] Rash, p. 1.

[40] Fred H. Cate, "Global Information Policymaking and Domestic Law," available from: <http://www.law.indiana.edu/glsj/vol1/cate.html>; Internet; accessed 11 January 1998.

[41] Rash, p. 1.

[42] Stallings, William, p. xxi.

[43] Graham, Bradley, p. 1.

[44] "The President's Commission on Critical Infrastructure Protection," Oct 97, available from: <http://www.pccip.gov/sumarry.html>; Internet; accessed 20 January 1998.

[45] Ibid., p. 89.

[46] Clipper Chip is a hardware product of the National Security Agency. It is a computer chip that encodes voice and data communications (i.e. telephones, fax machines, and modems). The difference in clipper chip and other encryption devices "is that the chip has a trap door that [law enforcement, with a search warrant] can open to wiretap clipper equipped devices." Stallings, p. 213.

[47] Biometrics is a type of authentication using fingerprints, voiceprints, palm prints, retinal scans, and other physical/biological signatures of an individual. Howard, Garry S., Introduction to Internet Security from Basics to Beyond. Rocklin, CA: Prima Publishing, 1995, p.125.

[48] Statement by the National Research Council on computer security, "Computers at Risk: Safe Computing in the Information Age," (National Academy Press, 1991), 7.

[49] "National Nightmares," available from: <http://www.infowar.com/class 3/class3 081897.html>; Internet; accessed 4 December 1997.

BIBLIOGRAPHY

Aldrich, Richard W., "The International Legal Implications of Information Warfare," Apr 96. Available from <http://www.usafa.af.mil/inss/ocp9.htm>. Internet. Accessed 5 January 1998.

Alexander, Michael. Net Security: Your Digital Doberman. NC: Ventana Communications, 1997, p. 73.

Anderson, Kent, "Criminal Threats to Business on the Internet," 23 Jun 97, p. 2. Available from <http://www.aranet.com/~kea/papers/whitepaper.shtml>. Internet. Accessed 5 January 1998.

"Apocalypse Explained," CNET, 1997. Available from <http://zeppo.cnet.com/Content/features/Dlife/apocalypse /ss02a.html>. Internet. Accessed 9 October 1997.

Basken, Paul, "Wide Effort Urged to Protect Computers," 9 Oct 97, Washington, D.C. Available from <http:// www.infowar.com/civil De/civil 101397.html-ssi>. Internet. Accessed 12 December 1997.

"Cyber Threats." Available from <http://www.infowar.com/ hackers/hack.html>. Internet. Accessed 26 march 1998.

Devost, Matthew G., Houghton, Brian K., Pollard, Neal A., members of The Terrorism Research Center. From the article "Information Terrorism: Can You Trust Your Toaster." Available from <http://www.terrorism.com/ Terrorism/itpaper.html>. Internet. Accessed 16 November 1997.

Devost, Matthew G., Houghton, Brian K., Pollard, Neal A., "Information Terrorism: Political Violence in the Information Age." Available from <http://www.terrorism. Com/denning.html>. Internet. Accessed 11 January 1998.

From e-mail message entitled, "A Quote for the Ages," 4 September 1997. Available from <wysiwyg://125/http: //www.infowar.com/hacker/hack_090897.html-ssi>. Internet. Accessed 23 November 1997.

Field, Richard L. "Electronic Banking: Banking Has Important Stake in Unfolding Cryptography Regulations."

Available from <http:www.ctr.columbia.edu/vii/crypto/ R1f2.htm>. Internet. Accessed 12 December 1997.

Goncalves, George, "Terrorist Group Profiles: Red Brigade," Last Update, 2 Mar 97. Available from <http://www.milnet com/milnet/tgp/data/br.htm>. Internet. Accessed 27 March 1998.

Howard, Garry S. Introduction to Internet Security From Basics to Beyond. Rocklin, CA: Prima Publishing, 1995, p. 249.

Joint Security Commission, "Technology Report on Cyber-terrorism." 1994 p.1. Available from <http://www.mvhs .srusd.k12.ca.us/~kwade/techreport.html>. Internet. Accessed 11 January 1998.

Kanaley, Reid, from the article "Analyst Finds U.S. Treasury, Military Computers Vulnerable to Infowar." Available from <wysiwyg://184/http://www.infowar.com/ Civil_de/civil_i.html-ssi>. Internet. Accessed 27 March 1998.

McLennan, James W. "Battlefield of the Future." Available From <http://www.cdsar.af.mil/battle/chp7.html>. Internet. Accessed 16 November 1998.

Howard, Garry S., Introduction to Internet Security from Basics to Beyond. Rocklin, CA: Prima Publishing, 1995, p.354.

"National Nightmares." Available from <http://www.infowar .com/class_3/class3_081897.html>. Internet. Accessed 12 December 1997.

"New Security Threats Rest in Cyber Terrorism," 3 Feb 1997. Available from <http://www.infowar.com/civil_de/ civil_c.html-ssi>. Internet. Accessed 18 December 1997.

Panska, Elizabeth. PC Novice Guide to the Web. Lincoln, NE: Peed Corporation, 1996, p. 6.

Phinney, David, "Electronic Plan of Attack." 20 Oct 1997, p.1. Available from <http://www.abcnews.aol.com/sections

/us/cyberterror1020/index.html>. Internet. Accessed 28 March 1998.

Platzer, Douglas. "The Future of Terrorism," March 1997. Available from <http://www.terrorism.com/terrorism>. Internet. Accessed 20 January 1998.

"The President's Commission on Critical Infrastructure Protection, Report Summary." Oct 97. Available from <http://www.pccip.gov/sumarry.html>. Internet. Accessed 20 November 1997.

Rasch, Mark D. The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues, Chapter 11, "Criminal Law and the Internet." The Computer Law Association, 1996, p.1.

REUTERS, "FBI Chief Calls for Computer Crime Crackdown." 28 Oct 97. Available from <wysiwyg://65/http://www.infowar.com/class_2103097b.html-ssi>. Internet. Accessed 20 November 1997.

Sloan, Steven. "Terrorism: How Vulnerable is the United States." Paper. "Terrorism: National Security Policy and the Home Front, edited by Stephen Pelletiere. The Strategic Studies Institute, U.S. Army War College, May 1995. Available from <http://www.terrorism.com/terrorism/sloan.html>. Accessed 20 November 1997.

Stallings, William. Internet Security Handbook. Westport, CT: IDG Books Worldwide, 1995, p.

DOCUMENT 3

Information Assurance Technology Analysis Center. Information Assurance Tools Report. Vulnerability Analysis

AD-A350433

1998

Information Assurance Technology Analysis Center
McLean, Virginia

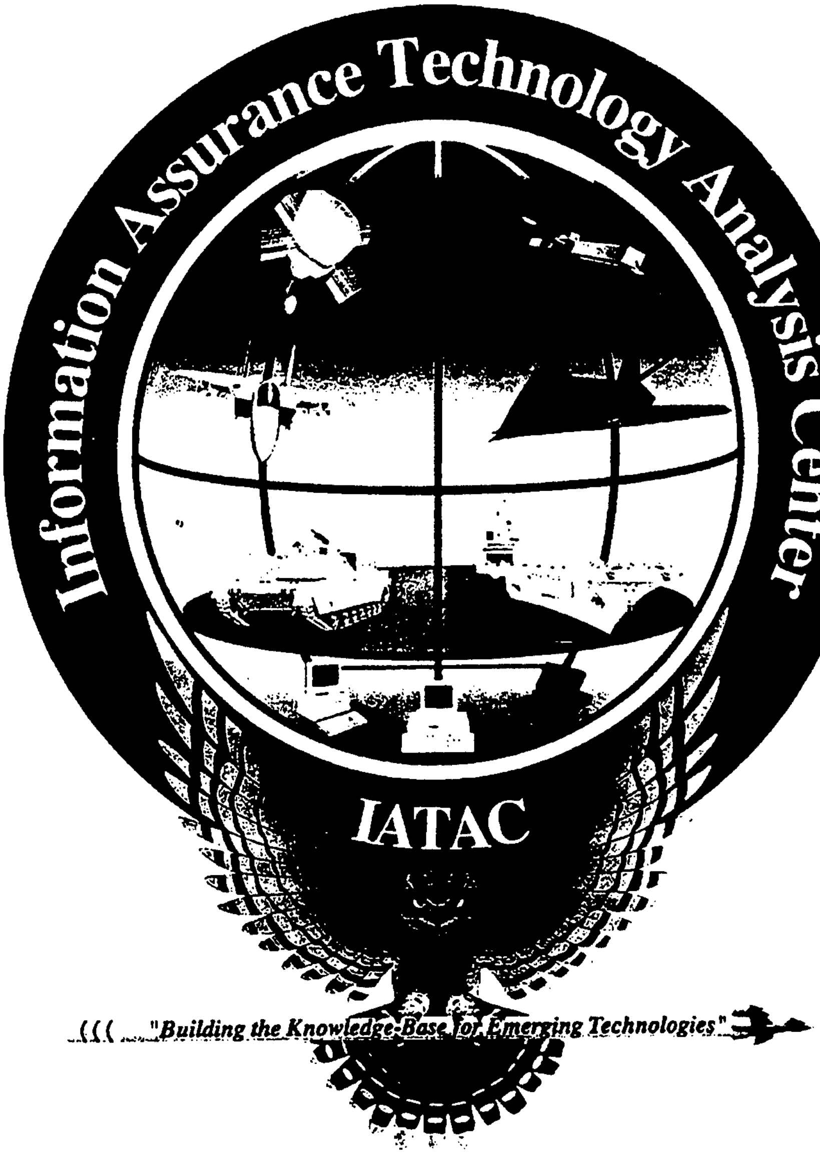
Information Assurance Technology Analysis Center

Information Assurance Tools Report

Spring 98

DISTRIBUTION STATEMENT A - Approved for public release, distribution is unlimited

VULNERABILITY ANALYSIS


Information Assurance Technology Analysis Center
IATAC
"Building the Knowledge-Base for Emerging Technologies"

8283 Greensboro Drive, Allen 663
McLean, VA 22102-3838

703.902.3177

Fax 703.902.3425

STU-III 703.902.5869

STU-III Fax 703.902.3991

E-mail iatac@dtic.mil

http://www.iatac.dtic.mil

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** Spring 1998	**3. REPORT TYPE AND DATES COVERED** Spring 1998

4. TITLE AND SUBTITLE
Information Assurance Technology Analysis Center
Information Assurance Tools Report
Vulnerability Analysis

5. FUNDING NUMBERS
SPO700-97-R-0603

6. AUTHOR(S)
IATAC

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC/AI
8725 John J. Kingman Road, #0944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
N/A

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This report provides an index of vulnerability analysis tool descriptions contained in the IATAC Information Assurance Tools Database. This report summarizes pertinent information, providing users with a brief description of available tools and contact information. It does not endorse or evaluate the effectiveness of each tool. As a living document, this report will be updated periodically as additional information is entered into the Information Assurance Tools Database.

14. SUBJECT TERMS

Vulnerability Analysis

15. NUMBER OF PAGES
42

16. PRICE CODE None

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** U

TABLE OF CONTENTS

INTRODUCTION

The Information Assurance Technology Analysis Center (IATAC) is a Department of Defense (DoD) sponsored Information Analysis Center (IAC) that provides a central point of access for scientific and technical information (STINFO) regarding information assurance (IA) technologies, system vulnerabilities, research and development, and models and analyses. The overarching goal of the IAC is to aid in developing and implementing effective defenses against information warfare attacks. IATAC basic services include support for user inquiries, analysis, maintenance, and growth of the IA library; IA database operations; development of technical and state-of-the-art reports; and promotional awareness activities, such as newsletters, conferences, and symposia.

IACs are staffed by scientists, engineers, and information specialists. Each IAC establishes and maintains comprehensive knowledge bases that include historical, technical, scientific, and other data and information collected worldwide. Information collections span a wide range of unclassified, limited distribution, and classified information appropriate to the requirements of sponsoring technical communities. IACs also collect, maintain, and develop analytical tools and techniques including databases, models, and simulations. Their collections and products represent intensive evaluation and screening efforts to create authoritative sources of evaluated data.

This report addresses the contents of the Information Assurance Tools Database, one of the knowledge bases maintained by IATAC. This database hosts information on intrusion detection, vulnerability analysis, firewalls, and antivirus software applications. Information for this database is obtained via open-source methods, including direct interface with various agencies, organizations, and vendors.

PURPOSE

This report provides an index of vulnerability analysis tool descriptions contained in the IATAC Information Assurance Tools Database. This report summarizes pertinent information, providing users with a brief description of available tools and contact information. It does not endorse or evaluate the effectiveness of each tool.

As a living document, this report will be updated periodically as additional information is entered into the Information Assurance Tools Database. Technical questions concerning this report may be addressed to James Green at (703) 902-4887 or iatac@dtic.mil.

SCOPE

Currently the IATAC database contains descriptions of 35 tools that can be used to support vulnerability and risk assessment. Vulnerability analysis tools are programs that help automate the identification of vulnerabilities in a network or system. Vulnerabilities can be defined as weaknesses in a systems security scheme exploitation of which would negatively affect the confidentiality, integrity, or availability of the system or its data. The type and level of detail of information provided among tools varies greatly. Although some can identify only a minimal set of vulnerabilities, others can perform a greater degree of analysis and provide detailed recommended countermeasures. More recently developed tools provide user-friendly front ends and sophisticated reporting capabilities. The majority of the tools identified in the Information Assurance Tools Database are available on the Internet, and many are used by crackers in the first stage of an attack: vulnerability information gathering. Penetration tools, which perform destructive actions (i.e., denial of service attacks), are excluded from this category. Sniffers, and Trojan horse programs are also excluded from this category. Although many network utilities (i.e., host, finger) are valuable in identifying vulnerabilities on a host, they are often an automated component of vulnerability analysis tools, and therefore are not individually described in the database.

The database includes commercial products, individual-developed tools, government-owned tools, and research tools. The database was built by gathering as much open-source data, analyzing that data, and summarizing information regarding the basic description, requirements, availability and contact information for each vulnerability analysis tool collected. Generally, the commercially developed products are available. The government and academic tools, however, are reserved for specific projects and organizations. The research group or university determines, on an individual case basis, the availability of these research tools. These tools are included in the database solely to provide information regarding existing approaches for vulnerability analysis.

DATABASE FORMULATION

This section discusses the approach and methodology used for identifying and collecting the selected tools, the classification of each type, tool sources, and the structure of the database.

TOOL COLLECTION

Information for each tool was collected by leveraging existing community relationships. Collection activities included Internet searches to identify additional corporations, government agencies, professional organizations, and universities with involvement in vulnerability analysis. Industry professionals were consulted for information and suggestions for identifying and collecting available tools.

TOOL CLASSIFICATION

The vulnerability analysis tools described in the IATAC Information Assurance Tools Database fall within one or more of the following five classes:

Simple Vulnerability Identification and Analysis A number of tools have been developed that perform relatively limited security checks. These tools may automate the process of scanning Transmission Control Protocol/Internet Protocol (TCP/IP) ports on target hosts, attempting to connect to ports running services with well-known vulnerabilities and recording the response. They also may perform secure configuration checks for specific system features (e.g., network file system [NFS] configuration, discretionary access control [DAC] settings). The user interface of these tools is likely to be command-line based, and the reporting may include limited analysis and recommendations. These tools are also likely to be "freeware."

Comprehensive Vulnerability Identification and Analysis More sophisticated vulnerability analysis tools have been developed that are fairly comprehensive in terms of the scope of vulnerabilities addressed, the degree of analysis performed, and the extent of recommendations made to mitigate potential security risks. Many of these tools also provide a user-friendly graphical user interface.

War Dialers A war dialer consists of software that dials a specific range of telephone numbers looking for modems that provide a login prompt. The tools, at a minimum, record the modem numbers and login screen, but can also be configured to attempt brute force, dictionary-based, login attempts. The value of these tools to a system administrator is that they automate the process of identifying potential "back doors" in a network. Some of the tools described above in the "Comprehensive Vulnerability Identification and Analysis" category include war dialers.

Password Crackers Password cracker tools attempt to match encrypted forms of a dictionary list of possible passwords with encrypted passwords in a password file. This is possible because the algorithm used to encrypt operating systems' passwords is public knowledge. These tools support system administrators by allowing them to enforce password selection policies.

Risk Analysis Tools Risk analysis tools typically provide a framework for conducting a risk analysis but do not actually automate the vulnerability identification process. These tools may include large databases of potential threats and vulnerabilities along with a mechanism to determine, based on user input, cost-effective solutions to mitigate risks. The vulnerabilities identified using a true "vulnerability analysis" tool may be fed into a risk analysis tool.

TOOL SOURCES

Tools and information were identified from a number of sources. A representative sampling of these sources includes the following:

COMMERCIAL

AXENT Technologies, Inc.

Bellcore

Internet Security Systems

Intrusion Detection, Inc.

NETECT, Inc.

RiskWatch

Secure Networks Incorporated (SNI)

Somarsoft, Inc.

The Mitre Corporation

Trident Data Systems

WheelGroup Corporation*

* *On March 12, 1998, Cisco Systems completed its acquisition of WheelGroup Corporation.*

GOVERNMENT AND PROFESSIONAL AGENCIES AND RESEARCH CENTERS

ACM SIGSAC (Special Interest Group on Security, Audit, and Control)

Air Force Information Warfare Center

Defense Advanced Research Projects Agency (DARPA)

Center for Secure Information Systems (CSIS) at George Mason University

Central Intelligence Agency

COAST Project at Purdue University

Computer Security Research Laboratory at University of California at Davis

Computer Security Technology Center at Lawrence Livermore National Laboratory

Computing Professionals for Social Responsibility (CPSR)

Defense Information Systems Agency (DISA)

Department of Energy, Computer Incident Advisory Capability (CIAC)

IEEE-CS Technical Committee on Security and Privacy

IFIP Technical Committee 6 (Communication Systems)

IFIP Technical Committee 11 on Security and Protection in Information Processing

IFIP Working Group 11.3 on Database Security

IFIP Working Group 11.4 on Network Security

Information Sciences Institute, University of Southern California School of Engineering

Information Security Research Centre at Queensland University of Technology, Australia

Information Systems Audit and Control Research at CalPoly Pomona

Institute for Computer & Telecommunications Systems Policy at The George Washington University

International Association for Cryptologic Research

International Computer Security Association (ICSA)

Lawrence Berkeley National Laboratory

Los Alamos National Laboratory

National Institute of Standards and Technology (NIST) Computer Systems Laboratory

National Security Agency

Navy Research Laboratory Center for High Assurance Computer Systems (Naval Research Laboratory)

Navy Space and Naval Warfare Systems Command (SPAWAR)

SIRENE: SIcherheit in REchnerNEtzen (Security in Computer Networks) at the University of Hildesheim/IBM Zurich

Texas A&M University

U.S. Army Office of the Director of Information Systems for Command, Control, Communications, and Computers (ODISC4)

USENIX & System Administrators' Guild (SAGE)

FIRST (FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS)

Air Force Computer Emergency Response Team (AFCERT)

Army Computer Emergency Response Team (ACERT)

Australian Computer Emergency Response Team (AUSCERT)

CERT Coordination Center, Carnegie Mellon University

Computer Emergency Response Team for the German Research Network (DFN-CERT), German Federal Networks CERT, Germany

Computer Incident Advisory Capability (CIAC), U.S. Department of Energy

NASA Automated Systems Incident Response Capability (NASIRC)

Naval Computer Incident Response Team (NAVCIRT)

Purdue University Computer Emergency Response Team (PCERT)

SURFnet Computer Emergency Response Team (CERT-NL), Netherlands

Swiss Academic and Research Network CERT, Switzerland (SWITCH-CERT)

DATABASE STRUCTURE

The fields of the database include the following:

Title Name and abbreviation associated with the tool

Author Developer of the tool

Source Uniform resource locator (URL) of the primary source for obtaining the tool

Keyword Terms used to reference the tools using the database search engine

Contact Information Name, organization, telephone, facsimile, e-mail, and URL information for additional tool information

Abstract Brief description of the primary features of the tool

Requirements System requirements for operating the tool

Availability Accessibility information including procedures and pricing in some cases

TOOL SELECTION CRITERIA

The selected tools satisfy the following three criteria:

Definition These tools satisfy the objective, approach, and methodology of an vulnerability analysis tool based on the definition of vulnerability.

Specificity to Vulnerability Analysis The primary function of these tools is vulnerability analysis. They may also be used during the early stages of a penetration attack to identify the target system's weaknesses and help fine-tune the attack. However, penetration test tools, whose primary purpose is to exploit identified vulnerabilities and cause damage or destruction to the target system, have been excluded.

Current Availability These tools are currently available from the Government, academia, or commercial sources, or as freeware on the Internet.

RESULTS

The research for this report identified 35 vulnerability analysis tools currently being used and available. Appendix A includes complete database output for each tool. The content of Appendix A mirrors the database structure as defined in the "Database Structure" section of this report. The following summary chart provides the name, keywords, and a description of each tool.

Title	Source Type	Attributes	Contact Organization	E-mail	URL
Ballista	Commercial	comprehensive vulnerability analysis	Secure Networks Inc.	sales@secnet.com	http://www.secnet.com/
CheckXusers	Individual	simple vulnerability analysis	Bob Vickers	R.Vickers@ulcc.ac.uk	http://www.ulcc.ac.uk/
Chkacct	Individual	simple vulnerability analysis	ShabbirSafdar	shabbir@panix.com	http://www.panix.com/ ~shabbir
CONNECT	Individual	simple vulnerability analysis	unknown	unknown	http://www.giga.or.at/pub/ hacker/unix
COPS(Computer Oracle and Password System)	Individual	comprehensive vulnerability analysis	DanFarmer	security@earthlink.net	http://www.earthlink.net/ company/farmer.html
CPM (Check Promiscuous Mode)	Academia	simple vulnerability analysis	CERT Coordination Center	cert@cert.org	http://www.cert.org/ contactinfo.html
Crack	Individual	password cracker	Alec Muffett	alec.muffet@uk.sun.com	http://www.users.dircon.co. uk/~crypto/index.html
Domain Obscenity Control(DOC)	Individual	simple vulnerability analysis	Steve Hotz	shotz@pollux.usc.edu	http://www.isi.edu/
DumpAcl	Commercial	simple vulnerability analysis	Somarsoft, Inc.	info@somarsoft.com	http://www.somarsoft.com/
Expert System for Progressive Risk Identification Techniques (ESPRIT)	Government	risk analysis	Rickey Roach	roachr@ncr.disa.mil	http://www.westhem.disa.mil/ ~WEY/esprit/
ICE-PICK	Government	comprehensive vulnerability analysis	Space and Naval Warfare Systems Center	questions@infosec. navy.mil	http://infosec.navy.mil/ ICEPICK/
IdentTCPscan	Individual	simple vulnerability analysis	David Goldsmith	daveg@escape.com	http://www.giga.or.at/pub/ hacker/unix
InternetScanner	Commercial	comprehensive vulnerability analysis	Patrick Taylor	info@iss.net	http://www.iss.net
Kane Security Analyst (KSA)	Commercial	misuse detection, system monitoring, comprehensive vulnerability analysis	DanielDorr	info@intrusion.com	http://www.intrusion.com/ contact.htm
L0PHTCrack	Commercial	password cracker	L0PHT Heavy Industries	info@L0pht.com & admin@L0pht.com	http://www.L0pht.com/ L0phtcrack/
Netective	Commercial	simple vulnerability analysis	NETECT Inc.	sales@netect.com	http://www.netect.com
NetRecon	Commercial	comprehensive vulnerability analysis	AXENT Technologies, Inc.	sundav@axent.com	http://www.axent.com/
NetSonar	Commercial	comprehensive vulnerability analysis	Joel McSarland	info@wheelgroup.com	http://www.wheelgroup.com/ contact/1contact.html
Network Security Scanner(NSS)	Individual	comprehensive vulnerability analysis	Douglas O'Neal	Doug.ONeal@jhu.edu	http://www.jhu.edu/
Nfsbug	Individual	simple vulnerability analysis	LeendertvanDoorn	leendert@cs.vu.nl	http://www.asmodeus.com/ar chive/Xnix/nfsbug/nfsbug.c
Omniguard/ESM	Commercial	comprehensive vulnerability analysis	AXENT Technologies, Inc	info@axent.com	http://www.axent.com/
Perl Cops	Individual	comprehensive vulnerability analysis	DanFarmer	security@earthlink.net	http://www.earthlink.net/ company/farmer.html
PINGWARE	Commercial	comprehensive vulnerability analysis	Bellcore	telecom-info@bellcore.com	http://telecom-info.bellcore.com/
RiskWatch v7.1	Commercial	risk analysis	Caroline R. Hamilton	riskwatch@riskguard. com	http://www.riskguard.com/ prod01.htm
Security Analysis Tool for Auditing Networks(SATAN)	Individual	comprehensive vulnerability analysis	DanFarmer	security@earthlink.net	http://www.earthlink.net/ company/farmer.html
Secure Sun	Individual	simple vulnerability analysis	David Safford	d-safford@tamu.edu	http://www.cs.tamu.edu/
Snoopy Tools	Commercial	comprehensive vulnerability analysis	W. Reid Gerhart	wrg@mitre.org	http://www.mitre.org/resource s/centers/infosec/infosec.ht ml
SPI-NET	Government	comprehensive vulnerability analysis	Sandy Spark	ciac@llnl.gov	http://ciac.llnl.gov

Title	Source Type	Attributes	Contact Organization	E-mail	URL
Strobe	Individual	simple vulnerability analysis	Julian Assange	strobe@suburbia.net proff@suburbia.net	ftp://coast.cs.purdue.edu/pub/tools/unix/strobe/
System Security Scanner	Commercial	comprehensive vulnerability analysis	Patrick Taylor	info@iss.net	http://www.iss.net
Tiger	Academia	comprehensive vulnerability analysis	Doug Schales	Doug.Schales@net.tamu.edu	http://www.cs.tamu.edu/
ToneLoc	Individual	war dialers	Minor Threat and Mucho Maas	mthreat@paranoia.com -or-mthreat@ccwf.cc.utexas.edu	ftp://ftp.paranoia.com/pub/toneloc/tl110.zip
Trident Information Protection Toolbox	Commercial	risk analysis	Brian Finan	Brian_Finan@tds.com	http://www.tds.com/tb/index.html#anal
Value of Information Structured Analysis of Risk Tool (VISART)	Government	risk analysis	Dr. Donald R. Peeples	n/a	http://www.nsa.gov/
Xscan	Individual	simple vulnerability analysis	unknown	pendleto@math.ukans.edu	http://www.giga.or.at/pub/hacker/unix

TITLE

Ballista

AUTHOR

Secure Networks Inc.

SOURCE

http://www.secnet.com/nav1b.html

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Alfred Huger
Secure Networks Inc.
Suite 330, 1201 5th Street SW
Calgary, Alberta CANADA T2R-0Y6
Telephone: 403.262.9211
Facsimile: 403.262.9221
E-mail: sales@secnet.com
URL: http://www.secnet.com/

REQUIREMENTS

Solaris 2.5-2.6, Linux 2.x, BSDI 2.x, OpenBSD 2.x, FreeBSD 2.x, Windows NT 4.0

AVAILABILITY

Commercially available from http://www.secnet.com/. Evaluation copy available from http://www.secnet.com/nav1b.html. Licensing is based on a single host or specific addresses. Up to 10 addresses cost $150, up to 50 cost $350.

ABSTRACT

Ballista is a network security auditing tool used to discover security weaknesses in networked environments. Ballista uses extensive domain name system (DNS) auditing to map intranets and perform port scans. Vulnerability checks include file transfer protocol (FTP), Web Servers, Sendmail, RPC, NFS, NetBIOS, and network devices such as routers and bridges. Ballista also allows users to determine whether the filters of a firewall are securely configured and have password-guessing routines.

Secure Networks has developed a customizable tool included with Ballista, the Custom Auditing Packet Engine (CAPE). CAPE can perform complex protocol-level spoofing and attack simulations. CAPE also enables users to generate tool-sets onthefly to address unique network implementations. It can use custom scripts to verify the integrity of Access/Choke routers, filtering firewalls (statefull inspection or otherwise), etc. This modular architecture also allows Secure Networks to update Ballista easily and efficiently. Ballista's biweekly updates include new vulnerability checks and features.

TITLE

CheckXusers

AUTHOR

Bob Vickers

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/unix/

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

Bob Vickers
University of London Computer Centre
20 Guilford Street
London ENGLAND WC1N 1DZ
Telephone: 0171.692.1000
Facsimile: 0171.692.1234
E-mail: R.Vickers@ulcc.ac.uk
URL: http://www.ulcc.ac.uk/

REQUIREMENTS

UNIX (Perl script); no special privileges; netstat command in PATH variable.

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/pub/tools/unix/checkXusers.Z

ABSTRACT:

CheckXusers identifies users logged onto the current machine from insecure X servers. It enables system administrators to determine whether users are exposing themselves, and hence the system, to unacceptable risks. It should be run from an ordinary user account, not root. It assumes that the netstat command is somewhere in the PATH prior to execution.

CHKACCT

TITLE

Chkacct

AUTHOR

Shabbir Safdar

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/unix/chkacct/

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

Shabbir Safdar
The Voters Telecommunications Watch
233 Court Street #2
Brooklyn, NY 11201
Telephone: 718.596.2851
Facsimile: n/a
E-mail: shabbir@panix.com
URL: http://www.panix.com/~shabbir

REQUIREMENTS

UNIX (Perl script); Audits account from which it is run.

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/ pub/tools/unix/chkacct/chkacct.v1.1.tar.Z

ABSTRACT:

Chkacct was designed to complement tools like COPS and Tiger that check for configuration problems in an entire system. Chkacct is designed to check the settings and security of the current user's account. It identifies potential problems with the accountìs security and provides explanations of how to fix them. It may be preferable to have a security administrator ask problem users to run chkacct rather than directly alter files in their home directories.

Chkacct allows the user to check the security of his or her account quickly. It can be run out of a crontab in "harmless" mode and the output mailed to the user.

Chkacct checks the home directory for certain important "dot" files as well as searching throughout the entire home directory for files with all-user write permissions.

TITLE

CONNECT

AUTHOR

Unknown

SOURCE

http://www.giga.or.at/pub/hacker/unix

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

Name:	Unavailable
Address:	Unavailable
Telephone:	Unavailable
Facsimile:	Unavailable
E-mail:	Unavailable
URL:	Unavailable

REQUIREMENTS

UNIX (C source code)

AVAILABILITY

Freely available from http://www.giga.or.at/pub/hacker/unix/connect.tar

ABSTRACT:

This /bin/sh shell script scans a range of Internet Protocol (IP) addresses for machines that offer the Trivial File Transfer Protocol (TFTP) service. Although typically disabled, this service is generally considered insecure and can be exploited to extract system files including /etc/passwd and other critical system files. If CONNECT finds a machine running TFTP, it will automatically attempt to download the /etc/passwd file to determine whether the system is vulnerable.

TITLE

Computer Oracle and Password System (COPS)

AUTHOR

Dan Farmer

SOURCE

ftp:// ftp.cert.org

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Dan Farmer
3100 New York Drive
Pasadena, CA 91107
Telephone: 626.296.2400
Facsimile: 626.296.4130
E-mail: security@earthlink.net
URL: http://www.earthlink.net/company/farmer.html

REQUIREMENTS

UNIX (Perl script)

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/ pub/tools/unix/cops/

ABSTRACT

Computer Oracle and Password System (COPS) is a security toolkit that examines a system for a number of known weaknesses and alerts the system administrator to them. In some cases it can automatically correct these problems. COPS identifies security vulnerabilities and checks for empty passwords in /etc/passwd, files with all-user write permissions, misconfigured anonymous ftp's, and many other area.

CPM

TITLE

Check Promiscuous Mode (CPM)

AUTHOR

CERT Coordination Center

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/unix/

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Telephone: 412.268.7090
Facsimile: 412.268.6989
E-mail: cert@cert.org
URL: http://www.cert.org/pub/aboutcert/contactinfo.html

REQUIREMENTS

UNIX (C source code), no special privileges

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/ pub/tools/unix/cpm/.

ABSTRACT

Check Promiscuous Mode (CPM) checks whether any network interface on a host is in promiscuous mode. A host in promiscuous mode can view all network traffic passing through its branch. CPM uses standard BSD UNIX socket (2) and ioct1(2) system calls to determine a system's configured network interfaces and reports whether any of the network interfaces are currently in promiscuous mode.

CPM identifies the number of interfaces found, the name of each interface, and whether each interface is in normal or promiscuous mode. It returns the number of discovered promiscuous interfaces as its exit status. No special privileges are required to invoke CPM.

TITLE

Crack

AUTHOR

Alec Muffett

SOURCE

ftp://ftp.cert.org/pub/tools/crack/

KEYWORD

password cracker

CONTACT INFORMATION

Alec Muffett
Sun Microsystems Ltd.
Sun House
306 Cambridge Science Park
Milton Road
Cambridge CB4 4WG
ENGLAND
Telephone: 01223.420421
Facsimile: 01223.420058
Email: alec.muffet@uk.sun.com
URL: http://www.users.dircon.co.uk/~crypto/index.html

REQUIREMENTS

UNIX (C source code, Perl script). Tested on Solaris, Linux, FreeBSD, NetBSD, OSF, and Ultrix. Root privileges to execute.

AVAILABILITY

Freely available from ftp://ftp.cert.org/pub/tools/crack/

ABSTRACT:

Crack is a password-cracking program with a configuration language that allows the user to program the types of guesses attempted. Crack is designed to quickly locate vulnerabilities in UNIX (or other) password files by scanning the contents of a password file and testing entries for weak (i.e., dictionary) passwords.

Crack helps the system administrator identify weak passwords by checking for various weaknesses and attempting to decrypt them. Systems employing shadowing password schemes are much harder to crack.

Crack's general procedure is to take as its input a series of password files and source dictionaries. It merges the dictionaries, turns the password files into a sorted list, and generates lists of possible passwords from the merged dictionary. Crack makes many individual passes over the password entries supplied as input. Each pass generates password guesses based on a sequence of rules.

Features include Eric Young's "libdes" encryption routines, an application programming interface (API) for ease of integration with arbitrary crypt() functions, API for ease of integration with arbitrary passwd file format, considerably better gecos-field checking, more powerful rule sets, ability to read dictionaries generated by external commands, better recovery mechanisms for jobs interrupted by crashes, improved control (e.g., disable during working hours). In addition, it comes bundled with Crack6 (minimalist password cracker) on with Crack7 (brute force password cracker).

TITLE

Domain Obscenity Control (DOC)

AUTHORS

Steve Hotz
Paul Mockapetris

SOURCE

http://csrc.nist.gov/tools/tools.htm

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

Steve Hotz
Paul Mockapetris
University of Southern California School of Engineering Information Sciences Institute
4676 Admiralty Way, Suite 1001
Marina del Rey, CA 90292-6695
Telephone: 310.822.1511
Facsimile: 310.823.6714
E-mail: shotz@pollux.usc.edu
URL: http://www.isi.edu/

REQUIREMENTS

UNIX (csh script)

Version 2.0 of the DNS query tool "dig" domain Internet groper

AVAILABILITY

Freely available at ftp://coast.cs.purdue.edu /pub/tools/unix/doc.2.0.tar.z

ABSTRACT:

Domain Obscenity Control (DOC) diagnoses misconfigured domains by sending queries to the appropriate domain name system (DNS) name servers and performing simple analysis on the responses. DOC verifies a domain's proper configuration and that it is functioning correctly. The domain name must be valid. Some changes to the script must be made including the first few aliases and pointers to directories.

DOC-V.2.0 is an initial implementation of an automated domain testing tool.

TITLE

DumpAcl

AUTHOR

Somarsoft, Inc.

SOURCE

http://www.somarsoft.com/

KEYWORD

simple vulnerability analysis

CONTACT INFORMATION

Somarsoft, Inc.
P.O. Box 642278
San Francisco, CA 94164-2278
Telephone: 415.776.7315
Facsimile: 415.776.7328
E-mail: info@somarsoft.com
URL: http://www.somarsoft.com/

REQUIREMENTS

Windows NT 3.51 or 4.0 (i386 and Alpha platforms). Targets Windows NT (any platform).

AVAILABILITY

Shareware version freely available from http://www.somarsoft.com/. Shareware version is fully functional except for printing. V2.7 adds enhancements and bug fixes for $99.

ABSTRACT:

Somarsoft DumpAcl dumps the permissions and audit settings for the Windows NT file system, registry, user/group information, and printers in a concise, readable, listbox format so the user can identify readily apparent security vulnerabilities.

Somarsoft DumpAcl provides a solution to the problem of having too many files and registry keys to manually check on a regular basis. Unnecessary system, file, and directory access can be identified from the tool's output.

TITLE

Expert System for Progressive Risk Identification Techniques (ESPRIT)

AUTHOR

Joint Information Service Center of DISA

SOURCE

http://www.westhem.disa.mil/~WEY/esprit/

KEYWORD

risk analysis

CONTACT INFORMATION

Rickey Roach
Defense Information Systems Agency
Alexandria, VA 22204
Telephone: 703.607.4215
Facsimile: n/a
E-mail: roachr@ncr.disa.mil
esprit@ncr.disa.mil
URL: http://www.westhem.disa.mil/~WEY/esprit/

REQUIREMENTS

IBM-compatible PC 386, MS-DOS version 3.3 or higher, 13 MB of disk space, 2 MB RAM

AVAILABILITY

Available to approved Government agencies from http://www.westhem.disa.mil/~WEY/ esprit/

ABSTRACT

ESPRIT was developed for the Joint Staff Support Center (JSSC) in support of its continuing efforts to define and develop cost-effective procedures to assist in performing risk analysis. ESPRIT is a risk analysis and risk management tool to aid Department of Defense (DoD) risk analysts in performing automated information systems (AIS) risk analysis.

ESPRIT checks for risk-management compliance and is an automated tool to conduct certification. It provides a detailed analysis of an information system in terms of assets, threats to assets, vulnerabilites, and countermeasure recommendations. ESPRIT analysis indicates the current security level and gathers data needed to select adequate and cost-effective safeguards. It includes a database of pre-ranked vulnerabilities in order of their relative severity (i.e., high, medium, or low). The program posts the ranking of each vulnerability identified on the target system.

ESPRIT's database also contains countermeasure statements and descriptions. With predefined links between the vulnerabilities and the appropriate countermeasures. Answers to the initial questionnaires trigger an automatic linkup between an inferred vulnerability and its associated appropriate countermeasure.

A userid and password must be obtained (this can be done from the Web page) to download the program from the Web site.

ICE-PICK

TITLE

ICE-PICK

AUTHOR

SPAWAR

SOURCE

http://infosec.navy.mil/ICEPICK/

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Commanding Officer
Code 72
Space and Naval Warfare Systems Center
Charleston SC (SPAWARSYSCEN)
P.O. Box 190022
North Charleston, SC 29419-9022
Telephone: 800.304.4636
Facsimile: n/a
E-mail: questions@infosec.navy.mil
URL: http://infosec.navy.mil/ICEPICK/

REQUIREMENTS

Version 1.2 - UNIX running Sunos 4.1.x, 4MB RAM; graphical interface such as Motif, Openwindows, or Xwindows; version 1.3 - Alpha Developments; portability to HP-UX version 10

AVAILABILITY

Available to approved Government agencies from ftp://infosec.navy.mil/pub/DOCs/navy /ice_req.DOC

ABSTRACT

ICE-PICK is U.S. Government property and is strictly controlled by SPAWAR for official Government use only. Unauthorized use, distribution, reproduction, or possession may be grounds for criminal prosecution including imprisonment. The complete ICE-PICK package is a security tool, for use by the system administrator tin identifying and fixing potential vulnerabilities.

ICE-PICK is an automated security tool used for evaluating the vulnerabilities of network-based systems that use TCP/IP. The tool is used to evaluate and rate the vulnerability of individual systems to various security threats that may be applied.

ICE-PICK is being distributed by the SPAWAR Systems Center Charleston SC to all Navy and Marine units. A Memorandum of Agreement must be signed by each requesting activity prior to release of the tool.

TITLE

IdentTCPscan

AUTHOR

David Goldsmith

SOURCE

http://www.giga.or.at/pub/hacker/unix

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

David Goldsmith

Address:	Unavailable
Telephone:	Unavailable
Facsimile:	Unavailable
E-mail:	daveg@escape.com
URL:	Unavailable

REQUIREMENTS

UNIX (C source code). Tested on BSDI, Linux 2.x, and SunOS 4.1.x.

AVAILABILITY

Freely available from http://www.giga.or.at/pub/hacker/unix/identTCPscan.c.gz

ABSTRACT

IdentTCP scans remote hosts for active Transmission Control Protocol (TCP) services. In addition, the tool attempts to determine the UID of the running processes. Processes that execute as root will be targeted first by system crackers, because any manipulation of those services is more likely to give root access to the system. System administrators can use this utility to determine which services may be targeted and then evaluate the necessity of running the service as root. Output is comprehensive and easy to read.

TITLE

Internet Scanner

AUTHOR

Internet Security Systems

SOURCE

http://www.iss.net/prod/isb.html

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Patrick Taylor
41 Perimeter Center East
Suite 660
Atlanta, GA 30346
Telephone: 770.395.0150
Facsimile: 770.395.1972
E-mail: info@iss.net
URL: http://www.iss.net

REQUIREMENTS

Windows NT 4.0, IBM AIX™ 3.25 and higher, HP-UX 9.05 and higher, Sun Solaris 2.3 and higher, Sun Solaris x86, SunOS 4.1.3 and higher, Linux 1.2x and 1.3x (with kernel patch), and Linux 1.3.7.6 and higher (no patch required). Disk space/memory requirements: Windows NT (10/24 MB); UNIX (5/24 MB).

AVAILABILITY

Commercial, single-host web scans cost approximately $1,500. Evaluation copy available from http://www.iss.net

ABSTRACT

The Internet Scanner tool set focuses on identifying and addressing network vulnerabilities. They perform scheduled and selective probes of network communication services, operating systems, key applications, and routers in search of common vulnerabilities that open the network to attack. Internet Scanner analyzes vulnerability conditions and provides sets of corrective action, trends analysis, conditional and configuration reports, and data sets.

Internet Scanner consists of three integrated modules for scanning intranets, scanning firewalls, and scanning Web servers. These modules are available singly, or as part of the Internet Scanner bundle.

Internet Scanner's intranet module is a network security assessment tool designed to automatically detect potential network vulnerabilities using an extensive battery of penetration tests. This graphical software utility provides a repeatable and reliable method of assessing the security configuration of systems.

Internet Scanner's firewall module helps maximize a firewall's protection by allowing the user to test for dozens of known vulnerabilities and misconfigurations. Its analysis tools and graphical user interface indicate where the firewall is at risk and recommend how to control the security exposure. Internet Scanner also provides "service" scans identifying all network services enabled across the firewall.

Internet Scanner's Web server module helps harden Web servers with a suite of analytical tools that reports potential vulnerabilities and misconfigurations and suggests methods of reducing system exposure. Internet Scanner audits and tests the operating system running the Web servers, the Web server application itself, and CGI scripts in the Web applications. Security vulnerabilities in the Web site are identified in a comprehensive Hyper-Text Markup Language (HTML) report describing the vulnerabilities along with recommended corrective actions.

KSA

TITLE

Kane Security Analyst (KSA)

AUTHOR

Intrusion Detection Incorporated

SOURCE

http://www.intrusion.com/product/ksa_nt.htm

KEYWORDS

misuse detection, system monitoring, comprehensive vulnerability analysis

CONTACT INFORMATION

Daniel Dorr
Intrusion Detection, Inc.
217 E 86th St., Suite 213
New York, NY 10028
Telephone: 212.348.8900.x302
Facsimile: 212.427.9185
E-mail: info@intrusion.com
URL: http://www.intrusion.com/contact.htm

REQUIREMENTS

Windows NT. Targets Windows NT and Novell Netware.

Root privileges

AVAILABILITY

Commercially available from http://www.intrusion.com

ABSTRACT:

KSA assesses the security status of a Novell and Windows NT network and generates reports in six areas: password strength, access control, user account restrictions, system monitoring, data integrity, and data confidentiality.

The database of known vulnerabilities that KSA uses contains password cracking tests, permissions across domains, C2 security, trust relationships, event logs, insecure partitions, audit policy compliance, uninterruptible power supply (UPS) status, excessive rights, registry security settings, guest ID configuration, and NT services.

New features include an interactive registry assessment, access control list (ACL) maps, and Kane File Rights for NTFS volumes. The Kane File Rights is an interactive tool included with the KSA that allows the user to automatically audit rights and privileges associated with various users, groups, and directories. The report generated by this audit includes percentages of compliance with the settings entered by the user.

TITLE

LOPHTCrack 2.0

AUTHOR

LOPHT Heavy Industries

SOURCE

http://www.L0pht.com/L0phtcrack/

KEYWORD

password cracker

CONTACT INFORMATION

L0pht Heavy Industries
P.O. Box 990857
Boston, MA 02199

Telephone:	Unavailable
Facsimile:	Unavailable
E-mail:	info@L0pht.com & admin@L0pht.com
URL:	http://www.L0pht.com/.

REQUIREMENTS

Windows 95/NT 4.0, source code available for UNIX (command line only). Targets Windows NT 4.0.

AVAILABILITY

Shareware with a 15-day free trial period, $50 registration fee.

ABSTRACT

This is a comprehensive password cracker for Windows NT system and local area network (LAN) manager passwords. The latest version has the builtin capability to extract encoded passwords from registry SAM files as well as directly from the system registry. Once passwords have been extracted, they are subject to a configurable brute force password attack.

TITLE

Netective

AUTHOR

NETECT Inc.

SOURCE

http://www.netect.com/

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

NETECT Inc.
212 Northern Avenue
West 1, Suite 300
Boston, MA 02210

Telephone:	617.753.7370
Facsimile:	617.753.7350
E-mail:	sales@netect.com
URL:	http://www.netect.com

REQUIREMENTS

SunOS 4.14, Solaris 2.5.1, HP UX 10.x, Windows NT. 50 MB free hard disk space, 64 MB minimum RAM, access to a local CD-ROM drive. JAVA-compatible UNIX, HTML browser, GUI (graphical user interface) for UNIX (e.g., X-Windows, Motif), root privileges.

AVAILABILITY

Commercially available from http://www.netect.com/

ABSTRACT

Netective identifies security vulnerabilities at both the operating system level and the network level. Netective validates the system using MD5 checksums and other security checks on system files, operating system patches, file permissions, and system passwords. Netective includes a dictionary-based password cracker.

Netective modules include the following:

The Network Module maps all ports to detect potential weak points. Each detected port is subjected to appropriate hacking attempts by the port checker. Special care is given to specific services such as NFS and RPC.

The Operating System Module checks system files, patches, MD5 checksums, permissions, and passwords across the system.

The Database Module contains a library of security vulnerabilities and their respective fixes and/or patches. It is updated regularly by NETECT.

A Graphical User Interface Module displays system status and analysis. Detected breaches and their recommended corrective actions are all presented in rich hypertext.

NETRECON

TITLE

NetRecon

AUTHOR

AXENT Technologies, Inc.

SOURCE

http://www.axent.com/netrecon/html/orderform.htm

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

AXENT Technologies, Inc.
2400 Research Boulevard
Rockville, MD 20850
Telephone: 301.258.5043
Facsimile: 301.330.5756
E-mail: sundav@axent.com
URL: http://www.axent.com/

REQUIREMENTS

Operates on Windows NT. Targets UNIX and Windows NT servers, NetWare networks, Windows workstations, mid-range systems, mainframes, routers, gateways, Web servers, firewalls, name servers, and others.

AVAILABILITY

Commercially available from http://www.axent.com/netrecon/html/orderform.htm and priced at $1,995 for limited scan of a single class C network or $9,995 for a license to scan an unlimited number of networks. Demo available from http://www.axent.com/netrecon/surveyde.htm.

ABSTRACT

OmniGuard/NetRecon runs on a Windows NT workstation and probes networks and network resources. NetRecon performs internal and external scans of the network. UltraScan exploits multiple protocols and methods to detect vulnerable network resources. NetRecon executes parallel scans of the network systems, devices, servers, firewalls, etc., for common vulnerabilities. NetRecon's probes are organized into a hierarchy. For example, one process looks for password information from an NIS server, another process tries to crack passwords, while a third looks for servers with rlogin (remote login) services to see whether the cracked user passwords will provide access.

A few of the vulnerabilities that NetRecon checks for include resources discovered, exec service enabled, smtp decode alias enabled, null session access obtained, user level access obtained, discovered system type, nis encrypted password obtained, password cracked using small/large dictionary, local disks mountable via smb, NetWare notification password trap possible, and port [number] active.

TITLE

NetSonar

AUTHOR

WheelGroup Corporation
Acquired by Cisco Systems on 3/12/98

SOURCE

http://www.wheelgroup.com/netsonar/sonar.html

KEYWORD

comprehensive vulnerability analysis

CONTACT INFORMATION

Joel McSarland
WheelGroup Corporation
13750 San Pedro, Suite 670
San Antonio, TX 78232
Telephone: 210.494.3383
Facsimile: 210.494.6303
E-mail: info@wheelgroup.com
URL: http://www.wheelgroup.com/contact/1contact.html

REQUIREMENTS

Solaris 2.5x or 2.6. Hardware: 32 MB RAM, 2 GB hard drive, TCP/IP network interface, CD-ROM drive, HTML browser

AVAILABILITY

Commercially available with an entry class "C" license starting at $2,995.

ABSTRACT

NetSonar is a vulnerability scanner and network mapping system. Using NetSonar from a central console, the user can assess the security state of an enterprise's entire network, track historical vulnerability trends, and create reports of potential security risks.

Launched from an intuitive graphical user interface at a central console, NetSonar runs in either manual or automatic mode. It can also run specialized profiles to look for certain sets of vulnerabilities, which enables the user to quickly determine whether the vulnerabilities previously detected still exist.

NetSonar can scan a large number of range of unspecified Internet Protocol (IP) addresses. NetSonar can comprehensively scan all systems on a network, including all firewalls, web servers, routers, switches, and other systems. NetSonar Entry provides all of the same capabilities as NetSonar but allows for unlimited scanning of only one specific class C network address range (up to 254 computer systems) assigned by the user during installation.

To protect against potential misuse of the product, all NetSonar scans are identified by an "electronic fingerprint" tied to the authorized, licensed user.

NOTE: On March 12, 1998, Cisco Systems completed its acquisition of WheelGroup Corporation.

TITLE

Network Security Scanner (NSS)

AUTHOR

Douglas O'Neal

SOURCE

ftp://jhunix.hcf.jhu.edu/pub/nss/README

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Douglas O'Neal
The Johns Hopkins University
3400 North Charles Street
Baltimore, MD 21218
Telephone: 410.516.8000
Facsimile: n/a
E-mail: Doug.ONeal@jhu.edu
URL: http://www.jhu.edu/

REQUIREMENTS

UNIX (Perl script), ftplib.pl

AVAILABILITY

Freely available from ftp://jhunix.hcf.jhu.edu/pub/nss

ABSTRACT

Network Security Scanner (NSS) scans individual remote hosts and entire subnets of hosts for various simple network security problems. The majority of the tests can be performed by any nonprivileged user on a typical UNIX machine. The only test currently implemented that requires root privileges is the check for a insecure hosts.equiv file. This test requires that a fake username (e.g., bin) be fed into rexec.

NSS will not create any files on remote machines nor will it run any nontrivial programs on remote machines.

The only nonstandard external program it invokes is ypx, a program that attempts to download the password map from a NIS server. Ypx was posted in comp.sources.misc and is archived in volume 40. NSS also requires the ftplib.pl package if running Perl version 4.x. Ftplib.pl is available from several Perl archives, for example ftp://anubis.ac.hmc.edu/pub/perl/library/ftplib.pl.gz

This program was developed on a DECstation 5000 running Ultrix 4.4. It has had superficial portability checks made under SunOS 4.1.3 and Irix 5.2, but extensive work has not been performed from those platforms.

TITLE

Nfsbug

AUTHOR

Leendert van Doom

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/unix/nfsbug/

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

Leendert van Doom
Department of Mathematics and
Computer Science
Vrije Universiteit
De Boelelaan 1081A
1081 HV Amsterdam, THE NETHERLANDS
Telephone: 31.20.444.7762
Facsimile: 31.20.444.7653
E-mail: leendert@cs.vu.nl
URL: http://www.asmodeus.com/
archive/Xnix/nfsbug/nfsbug.c

REQUIREMENTS

UNIX (C source code)

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu /pub/tools/unix/nfsbug/

ABSTRACT

Nfsbug checks for a variety of configuration errors in NFS, mountd, and portmapper daemons. Tests check for specific NFS problems and bugs such as finding worldwide-exportable file systems, determining whether the export list really works, determining whether file systems are mountable through the portmapper, guessing file handles, exploiting the mknod bug, and the uid masking exploit.

TITLE

OmniGuard/ESM

AUTHOR

AXENT

SOURCE

http://www.axent.com/

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

AXENT Technologies, Inc.
2400 Research Boulevard
Rockville, MD 20850

Telephone:	301.258.5043
Facsimile:	301.330.5756
E-mail:	info@axent.com
URL:	http://www.axent.com/support/support.htm

REQUIREMENTS

Extensive software platform support for manager and agent components: Windows NT, NetWare, VMS, IBM-AIX, HP-UX, SunOS, IRIX, and others.

AVAILABILITY

Commercially available from http://www.axent.com/product/esm/esm.htm

ABSTRACT:

Omniguard/Enterprise Security Manager (ESM) is a platform-independent security management tool that enables the user to manage and evaluate diverse systems according to unique, customizable security policies. It also has an application Programming interface (API) that can be used to customize and integrate security management for other security products, applications, and databases.

The ESM architecture has three components: the graphical user interface (GUI), manager, and agent. These three components are supported on multiple software platforms, although the GUI is limited to UNIX systems compatible with X-Windows, Windows 3.x, 95, and NT. Agents contain executable modules that perform security checking and correction (based on policies) at the server, workstation, database, or application level. Agents can be run manually or on an automated schedule. The manager and GUI serve as interfaces that manipulate agents. Managers can also be used to set and apply security policies such as account integrity, backup integrity, file access violations, file attributes, virus checking, proper login parameters, trivial passwords, system auditing, and e-mail holes. Reports can be generated from these results that show the percentage of network resources complying with a pre-determined policy.

TITLE

Perl Cops

AUTHOR

Dan Farmer

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/unix/cops-perl.tar.gz

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Dan Farmer
3100 New York Drive
Pasadena, CA 91107

Telephone:	626.296.2400
Facsimile:	626.296.4130
E-mail:	security@earthlink.net
URL:	http://www.earthlink.net/company/farmer.html

REQUIREMENTS

UNIX (Perl script)

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/pub/tools/unix/cops-perl.tar.gz

ABSTRACT

Perl Cops is a security toolkit that examines a system for a number of known weaknesses and alerts the system administrator to them. This is a smaller, Perl version of Computer Oracle and Password System (COPS).

The user can specify the target (uid or gid) on the command line, using the -l option to generate PAT for a goal, and use -f to preload file owner, group and mode information. This preloading is helpful in terms of speed and avoiding file system "shadows." Features include caches for the passwd/group file entries for faster lookups.

PINGWARE

TITLE

PINGWARE

AUTHOR

Bellcore

SOURCE

http://www.bellcore.com

KEYWORD

comprehensive vulnerability analysis

CONTACT INFORMATION

Bellcore
8 Corporate Place, PYA 3A-184
Piscataway, NJ 08854-4156
Telephone: 800.521.2673
Facsimile: 732.366.2559
Email: telecom-info@bellcore.com
URL: http://telecom-info.bellcore.com/

REQUIREMENTS

SunOS 4.1 or above, Solaris 2.3, HP-UX 9.x

AVAILABILITY

Commercially available from http://telecom-info.bellcore.com/. Refer to document number OOA-1005

ABSTRACT

PINGWARE systematically scans and tests all the systems on a Transmission Control Protocol/Internet Protocol (TCP/IP) based network from a single workstation. It checks for security vulnerabilities on the target system from the network (i.e., outside the system). It simulates an intruder by exploiting common configuration errors and known bugs in TCP/IP-based services to access the system from the network. It identifies the systems vulnerable to attack and generates a report detailing the weak points in the network.

Features include multiprocessing testing capability, network inventory, retrieval of key system files, reporting and results management. Vulnerability tests include finger, ftp, http, NFS, rlogin/rsh, rpcinfo, sendmail, tftp, xhost, and password cracking.

RiskWatch 7.1

TITLE

RiskWatch 7.1 for Information Systems

AUTHOR

RiskWatch

SOURCE

http://www.riskguard.com/prod01.htm

KEYWORDS

risk analysis

CONTACT INFORMATION

Caroline R. Hamilton
900 Bestgate Rd., Suite 210
Annapolis, MD 21401
Telephone: 410.224.4773
Facsimile: 410.224.4995
E-mail: riskwatch@riskguard.com
URL: http://www.riskguard.com/prod01.htm

REQUIREMENTS

Windows 3.1x, Windows for Workgroups, Windows 95, Windows NT 3.51 and 4.0

AVAILABILITY

Commercially available from http://www.riskguard.com/

ABSTRACT

RiskWatch 7.1 for Information Systems conducts automated risk analysis and vulnerability assessments of information systems, including data centers, application programs, facilities, networks, and field offices. RiskWatch uses data generated by the risk analysis to provide on-line risk management and generate a variety of reports. RiskWatch is completely customizable by the user, including allowing the user to create new asset categories, threat categories, vulnerability categories, safeguards, question categories, and question sets. Users can also automatically import questions and data created by other users into their analysis.

RiskWatch automatically creates questionnaire diskettes, which are used by respondents and returned to the risk analysis manager for processing. Diskettes are created by the RiskWatch software on high or low density 3.5" floppy diskettes. Executables for the diskettes are included on the diskette. Users may generate an unlimited number of questionnaire disks.

SATAN

TITLE

Security Analysis Tool for Auditing Networks (SATAN)

AUTHOR

Dan Farmer
Wietse Venema

SOURCE

http://www.fish.com/satan/

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Dan Farmer
3100 New York Drive
Pasadena, CA 91107
Telephone: 626.296.2400
Facsimile: 626.296.4130
E-mail: security@earthlink.net
URL: http://www.earthlink.net/
company/farmer.html

REQUIREMENTS

UNIX (Perl script, expect, C source code)

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/ pub/tools/unix/satan/

ABSTRACT

SATAN scans systems connected to the network noting the existence of well-known, often-exploited vulnerabilities. SATAN examines a remote host or set of hosts and gathers as much information as possible by remotely probing NIS, finger, NFS, ftp and tftp, rexd, and other services. This information includes the presence of various network information services as well as potential security flaws involving misconfigured setup and network services and known bugs in system or network utilities. It then can either report on these data or use an expert system to further investigate any potential security problems. SATAN consists of several sub-programs, each of which is an executable file that tests a host for a given potential weakness. Additional test programs can be used by including the executable in the main directory with the extension ".sat." The driver generates a set of targets (using DNS and a fast version of ping together to get "live" targets) and then executes each of the programs on each of the targets. Three depths of scans are offered: light, normal, and heavy. A data filtering/interpreting program analyzes the output and a reporting program produces formatted output.

SATAN has not been updated since its development (c. 1995) and may not be able to detect certain vulnerabilities. For additional information, see: CIAC Notes 95-07 & CIAC Notes 95-08.

TITLE

Secure Sun

AUTHOR

David Safford

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/unix/secure-sun-check

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

David Safford
Director, TAMU Supercomputer Center
Texas A&M University
College Station, TX 77843-0100
Telephone: 409.845.1004
Facsimile: 409.845.0727
Email: d-safford@tamu.edu
URL: http://www.cs.tamu.edu/

REQUIREMENTS

UNIX (shell script). Specific to SunOS 4.0.3 and 4.1.

No special privileges.

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/pub/tools/unix/secure-sun-check

ABSTRACT

This program checks for 14 common SunOS configuration security vulnerabilities. Each test reports its findings and offers to fix any discovered problems. The program must be run as root to fix any of the problems, but it can be run from any account by replying \'n\' to any fix requests. It has only been tested under SunOS 4.0.3 on Sun4, Sun3, and Sun386i machines.

The 14 checks made are: fix ttytab to disable b -s problem, check /etc/hosts.equiv either null or at least no +, disable tftp \(nonserver\), or add secure switch \(server\), fix rcp hole, check root\'s path for, check dirs in root\'s path not writeable by others, check that /etc/passwd on ypserver does not have client line, check that uucp decode alias is removed from /etc/aliases, check /etc/utmp is not world writeable, check that rexd is disabled in /etc/inetd.conf, disable login shell for uucp, check for null /.rhosts, check for accounts with no password, and check for back-door root accounts.

TITLE

Snoopy Tools

AUTHOR

The MITRE Corporation

SOURCE

http://infosec.nosc.mil/content.html

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

W. Reid Gerhart
The MITRE Corporation, MS: B325
202 Burlington Rd
Bedford, MA 01730-1420
Telephone: 617.271.3738
Facsimile: 617.271.3957
Email: wrg@mitre.org
URL: http://www.mitre.org/resources/centers/infosec/infosec.html

REQUIREMENTS

Operate on a host (with a network interface) running UNIX (C source code). Tested on SunOS 4.x. Graphical interface to Snoopy Tools, xsnoopy, runs under the X11 window system. Requires the Motif libraries and 10 MB of disk space to compile.

AVAILABILITY

Developed for NAVCOMSTAR Vulnerability Assessment, Department of the Navy Space and Naval Warfare Systems Command Naval Information Systems Security Office, PMW 161, Prepared by Michelle Gosselin, Dan Vukelich, Len LaPadula (Ed.), The MITRE Corporation. March 1996.

ABSTRACT

Snoopy Tools is a suite of programs that determine what network services are running under Transmission Control Protocol/Internet Protocol (TCP/IP) and attempt to exploit bugs in those services. Snoopy probes hosts across a network in a non-intrusive manner by acting as an unprivileged client of the various services that are probed. The only indications that Snoopy is running are a possible brief spike in network activity and the audit log entries maintained by the hosts' servers.

Snoopy remotely probes hosts to determine whether selected security flaws are present in TCP/IP network services. It can act as a network sniffer to capture Novell network passwords and can scan AppleTalk networks for any readable files.

When Snoopy finds a host running TFTP, it attempts to retrieve the password file for later use in a cracking attack. However, if the password file is "shadowed," meaning that the passwords were not contained in /etc/passwd but rather in a shadow password file, the opportunity to crack the passwords of valid system users is minimized.

TITLE

SPI-NET

AUTHOR

Sandy Spark

SOURCE

http://ciac.llnl.gov/cstc/spi/spinet.html

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Sandy Spark
Computer Incident Advisory Capability
University of California
Lawrence Livermore National Laboratory
7000 East Ave.
P.O. Box 808
Livermore, CA 94550
Telephone: 510.422.8193
Facsimile: 510.423.8002
Email: ciac@llnl.gov
URL: http://ciac.llnl.gov

REQUIREMENTS

UNIX (C source). Tested on HP-UX 10.x, IRIX 5.x, SunOS 4.x, and SunOS 5.x

AVAILABILITY

Free SPI-NET distributions are limited to U.S. Government agencies and to contractors to the U.S. Department of Energy and U.S. Department of Defense. Ongoing commercialization efforts preclude free distribution and use by private industry.

ABSTRACT

SPI-NET supports multihost system security inspections managed from a designated "command host." These inspections include access control testing, system file authentication, file system change detection, password testing, and common system vulnerability checks. SPI-NET supports flexible inspection specification and scheduling, and provides reasonable default settings. All SPI-NET command and data traffic is protected by public key encryption techniques.

The binary distributions come in two forms: The "Stand-Alone" binaries support the command-host installation and are required for at least one host in a SPI-NET security domain. The "Detached" binaries provide the capability to inspect additional remote host machines under the control of the command-host. Both Stand-Alone and Detached packages come with Installation/Setup scripts for ease of installation.

STROBE

TITLE

Strobe

AUTHOR

Julian Assange

SOURCE

ftp://suburbia.net:/pub/strobe.tgz

KEYWORDS

strobe vulnerability analysis

CONTACT INFORMATION

Julian Assange
PO Box 2031 Barker VIC 3122
AUSTRALIA
Telephone: n/a
Facsimile: 61.3.9819.9066
Email: strobe@suburbia.net
proff@suburbia.net
URL: ftp://coast.cs.purdue.edu/pub/tools/unix/strobe/

REQUIREMENTS

UNIX (C source code)

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/pub/tools/unix/strobe/strobe.tgz

ABSTRACT

Strobe is a network security tool that locates and describes all listening tcp ports on a (remote) host or on many hosts. Strobe approximates a parallel finite state machine internally. In nonlinear multihost mode, it attempts to apportion bandwidth and sockets among the hosts very efficiently. On a machine with a reasonable number of sockets, Strobe can port scan entire Internet sub-domains.

TITLE

System Security Scanner

AUTHOR

Internet Security Systems

SOURCE

http://www.iss.net/prod/isb.html

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Patrick Taylor
41 Perimeter Center East
Suite 660
Atlanta, GA 30346

Telephone:	770.395.0150
Facsimile:	770.395.1972
Email:	info@iss.net
URL:	http://www.iss.net

REQUIREMENTS

SunoS 4.1.3-4.1.4, Solaris 2.3-2.5.1, AIX 3.2.5-4.2, HP-UX 9.05-10.x, Irix 6.2-6.4, and Linux 1.2.13+.

AVAILABILITY

Commercial. $495 for a single server license or $3,500 for a 10-server license. Evaluation copy available from company at http://www.iss.net.

ABSTRACT

System Security Scanner assesses operating system configuration, file permissions and ownership, network services, account setups, program authenticity, and common user-related security issues such as guessable passwords.

System Security Scanner is part of the SAFE-suite line of adaptive security management solutions. These technologies give a thorough view of security threats and vulnerabilities in network traffic, Web sites, firewalls, and UNIX and Windows NT operating systems. Once vulnerabilities are identified, System Security Scanner prioritizes its findings by high, medium, or low levels of risk. It provides reports and appropriate corrective actions and generates scripts to automatically correct vulnerabilities.

System Security Scanner's open database structure and highly flexible report engine provide data in both management and implementation formats.

TITLE

Tiger

AUTHOR

Doug Schales

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/unix/tiger/

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Doug Schales
Department of Computer Science
Texas A&M University
College Station, TX 77843-3112
Telephone: 409.845.5098
Facsimile: 409.847.8578
Email: Doug.Schales@net.tamu.edu
URL: http://www.cs.tamu.edu/

REQUIREMENTS

UNIX (Bourne shell script, C source code)

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/ pub/tools/unix/tiger/

ABSTRACT

Tiger is used to check for security problems on a UNIX system. It scans system configuration files, file systems, and user configuration files for possible security problems and reports them. Tiger was originally developed to provide a check of UNIX systems on the Texas A&M campus that users wanted to access from off campus. (Clearance was provided through the packet filter.)

TITLE

ToneLoc

AUTHOR

Minor Threat and Mucho Maas

SOURCE

ftp.paranoia.com/pub/toneloc/tl110.zip

KEYWORD

war dialers

CONTACT INFORMATION

Name:	Unavailable
Address:	Unavailable
Telephone:	Unavailable
Facsimile:	Unavailable
Email:	mthreat@paranoia.com -or- mthreat@ccwf.cc.utexas.edu
URL:	http://oberon.ark.com/~john/ frozenhell/files.html

REQUIREMENTS

Windows 3.x/95/NT, DOS 6.x, modem

AVAILABILITY

Freely available from ftp://ftp.paranoia.com/pub/toneloc/tl110.zip

ABSTRACT:

This software is designed to scan a block of telephone numbers for an active dial-up service. This tool may be useful to administrators who are unsure whether possible back doors are present in their computer or telephone network.

TRIDENT INFORMATION PROTECTION TOOLBOX

TITLE

Trident Information Protection Toolbox

AUTHOR

Trident Data Systems

SOURCE

http://www.tds.com/tb/index.html

KEYWORDS

risk analysis

CONTACT INFORMATION

Brian Finan
10455 White Granite Drive, Suite 400
Oakton, VA 22124
Telephone: 703.383.3686
Facsimile: 703.383.3530
Email: Brian_Finan@tds.com
URL: http://www.tds.com/tb/index.html#anal

REQUIREMENTS

Operates on Windows 95 and NT 4.0

AVAILABILITY

Commercially available from http://www.tds.com/tb/index.html#anal

ABSTRACT

Trident's Toolbox is a set of three complementary tools that assist in protecting critical information assets. Toolbox is a more specific and advanced version of the company's highly successful NetRISK product.

The Trident Information Protection Toolbox includes: Trident Information Protection Analyst, a comprehensive risk management software for networks; Trident Information Protection Architect, an automated network mapping and security design; and Trident Information Protection Library, a comprehensive information security database.

Analyst automates the risk assessment process, provides summary and detailed reports of the security risks present in networks, and offers solutions for reducing those risks. The Architect automatically identifies and graphically maps all of the hardware, services, and dial-up modem entry points. Library is a comprehensive reference of current computer security information. Its relational database format allows access to Analyst and Architect. The Library contains an extensive inventory of computer vulnerabilities with appropriate safeguards or patches for each vulnerability.

TITLE

Value of Information Structured Analysis of Risk Tool (VISART)

AUTHOR

Dr. Donald R. Peeples

SOURCE

National Security Agency

KEYWORDS

risk analysis

CONTACT INFORMATION

Dr. Donald R. Peeples
National Security Agency (VI)
Ft. Meade, MD 20755-6755
Telephone: 410.859.4704
Facsimile: n/a
Email: n/a
URL: http://www.nsa.gov/

REQUIREMENTS

Tool is currently under development.

AVAILABILITY

Tool is currently under development

ABSTRACT

VISART is a risk management tool currently under development by Dr. Donald Peeples at NSA's Information Security systems Office (ISSO). This tool allows the user to analyze systems, their vulnerabilities, and possible threats, and quantify what types of countermeasures are justifiable in terms of cost. The process begins with the collection of data to describe baseline procedures (risks and probabilities), including total aggregated risk. Once this is completed, a set of appropriate countermeasures are suggested, and the tool can be rerun to determine actual effectiveness. (Cost is based on level of security.)

TITLE

XScan

AUTHOR

Unknown

SOURCE

http://www.giga.or.at/pub/hacker/unix

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

Name:	Unavailable
Address:	Unavailable
Telephone:	Unavailable
Facsimile:	Unavailable
Email:	pendleto@math.ukans.edu
URL:	Unavailable

REQUIREMENTS

Linux or SunoS, 4.1.4, X system (C source code)

AVAILABILITY

Freely available from http://www.giga.or.at/pub/hacker/unix/xscan.tar.gz

ABSTRACT

This utility scans a host, or a range of hosts, for unprotected X displays. If an unprotected display is discovered, this utility monitors that connection and logs all keystrokes made on the display. This is a useful tool to exploit passwords that may be obtained from the local machine or remote machine depending on what the scanned target is doing with the open display. System administrators can use this tool to determine whether users are adequately restricting those hosts that can connect to their active X sessions.

Information Assurance Technology Analysis Center

Information Assurance Tools Report   Spring 98

DISTRIBUTION STATEMENT A - Approved for public release, distribution is unlimited

VULNERABILITY ANALYSIS

DOCUMENT 4

Critical Factors in Cyberspace

AD-A325529

1997

U.S. Naval War College
Newport, Rhode Island

NAVAL WAR COLLEGE
Newport, R.I.

CRITICAL FACTORS IN CYBERSPACE

by
John Van Cleave
Lieutenant Commander, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: J a Van Cle

08 November 1997

Paper directed by
G. W. Jackson, Captain, U.S. Navy
Chairman, Department of Joint Military Operations

Mark Welch 6FEB97
Faculty Advisor Date
Mark Welch, Commander, U.S. Navy

Security Classification This Page REPORT DOCUMENTATION PAGE

1. **Report Security Classification:** UNCLASSIFIED

2. **Security Classification Authority:**

3. **Declassification/Downgrading Schedule:**

4. **Distribution/Availability of Report:** DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. **Name of Performing Organization:**
JOINT MILITARY OPERATIONS DEPARTMENT

6. **Office Symbol:** C

7. **Address:** NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. **Title** (Include Security Classification):

CRITICAL FACTORS IN CYBERSPACE (U)

9. **Personal Authors:**
JOHN A. VAN CLEAVE, LCDR, USN

10. **Type of Report:** FINAL

11. **Date of Report:** 7 FEBRUARY 1997

12. **Page Count:** 22

13. **Supplementary Notation:** A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. **Ten key words that relate to your paper:** CRITICAL FACTORS, CYBERSPACE, CRITICAL STRENGTHS, CRITICAL WEAKNESSES, CRITICAL VULNERABILITIES,

15. **Abstract:** Since WWII, warfare and conflict involving the United States, has taken on an "antiseptic" dimension. Conflicts have been resolved in far away places, separated by distance and a powerful military force able to project power and take the fight to the enemy. In doing so the U.S. has remained relatively immune to attacks on its own social, economic, political, and military infrastructures. But as the U.S. forges ahead into the information age, the global connectivity inherent in this transformation also brings about new vulnerabilities.

The vast advantages of space - the fabled "high ground" - including the civil and military capabilities it brings to the U.S will soon be overshadowed by what could be termed the "common ground", Cyberspace. In Cyberspace highly computerized and networked social, economic, political, and military infrastructures become intertwined, increasing their vulnerability to attack. This paper will explore some current and future challenges that must be considered carefully as we develop the new common ground in Cyberspace and the impact that cyber weapons will have in reshaping operational and strategic planning. It will also identify critical factors traditional in U.S. infrastructures that are increasingly vulnerable to attack through Cyberspace due to these new linkages.

Through the utility of Cyberspace, once secure lines of communication will lose the sanctuary created by strategic geography and a strong military force. It is now incumbent upon civil and military planners to recognize these emerging vulnerabilities and establish new "forces" and "objectives" which protect American interests in this new frontier. As they are presently configured, traditional military force may not be able to handle the new security challenges posed by Cyberspace.

16. **Distribution / Availability of Abstract:**	**Unclassified** X	**Same As Rpt**	**DTIC Users**

17. **Abstract Security Classification:** UNCLASSIFIED

18. **Name of Responsible Individual:** CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19. **Telephone:** 841-6461

20. **Office Symbol:** C

Security Classification of This Page Unclassified

Abstract of
Critical Factors in Cyberspace

Since WWII, warfare and conflict involving the United States, has taken on an "antiseptic" dimension. Conflicts have been resolved in far away places, separated by distance and a powerful military force able to project power and take the fight to the enemy. In doing so the U.S. has remained relatively immune to attacks on its own social, economic, political, and military infrastructures. But as the U.S. forges ahead into the information age, the global connectivity inherent in this transformation also brings about new vulnerabilities.

The vast advantages of space - the fabled "high ground" - including the civil and military capabilities it brings to the U.S. will soon be overshadowed by what could be termed the "common ground", Cyberspace. In Cyberspace highly computerized and networked social, economic, political, and military infrastructures become intertwined, increasing their vulnerability to attack. This paper will explore some current and future challenges that must be considered carefully as we develop the new common ground in Cyberspace and the impact that cyber weapons will have in reshaping operational and strategic planning. It will also identify critical factors traditional in U.S. infrastructures that are increasingly vulnerable to attack through Cyberspace due to these new linkages.

Through the utility of Cyberspace, once secure lines of communication will lose the sanctuary created by strategic geography and a strong military force. It is now incumbent upon civil and military planners to recognize these emerging vulnerabilities and establish new “forces” and “objectives” which protect American interests in this new frontier. As they are presently configured, traditional military force may not be able to handle the new security challenges posed by Cyberspace.

Introduction

With the possibility of resolving future conflicts by fighting in other than a "terrain-defined battlespace," some of the basic definitions of operational art will no doubt have to be expanded upon .[1] But first; what is Cyberspace? Some would say, "The sensation of place without location, or space without physicality, experienced while using global computer networks." [2] Joint Pub 1-02, the *DOD Dictionary of Military and Associated Terms*, makes no mention of Cyberspace. Definitions in various periodicals identify the Internet and the World Wide Web as vehicles which allow access into Cyberspace. Volume I of the *Joint Command and Control, Communications, and Computers Systems Descriptions* publication alludes to Cyberspace as it provides a synopsis on the capability of the up and coming Global Command and Control System (GCCS) which will provide the ability to "...pull information through a global, integrated infosphere." [3] What is important is the fact that through the utility of Cyberspace, computer systems will be "tied together" (networked) locally or globally. With the extensive integration of social, economic, political, and military information systems by such a vast network of computers and information sharing systems, the U.S. will no doubt benefit from the intrinsic advantages that shared information can provide. But these advantages are not without a cost. By their very nature of operation; these information systems have more global exposure than ever before, making them vulnerable to enemy deception, manipulation, and attack. [4]

Understanding the impact that Cyberspace has in exposing previously secure critical strengths, weaknesses, and vulnerabilities (critical factors) requires in part, a general overview of past conflicts and how they were fought. The United States' infrastructure has enjoyed the strategic luxury of being physically distanced from the enemy by vast expanses of ocean.

Coupled with a military force able to project power, the U.S. was fairly insulated from direct attacks on its home soil. The geography of the situation alone would probably be a deterrent considering the extensive lines of communication (LOC's) and logistic's sustainment required by an adversary in carrying out an attack. With the utility of Cyberspace, hurdles such as LOC's and complex logistics requirements for force sustainment can be bypassed. Figure (1) depicts the traditional U.S. security paradigm in which the military comes between the adversary and society. Through Cyberspace, sanctuary is lost as is illustrated in Figure (2).[5]

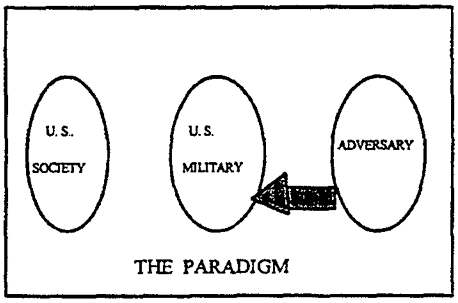


Figure 1. The Traditional Paradigm

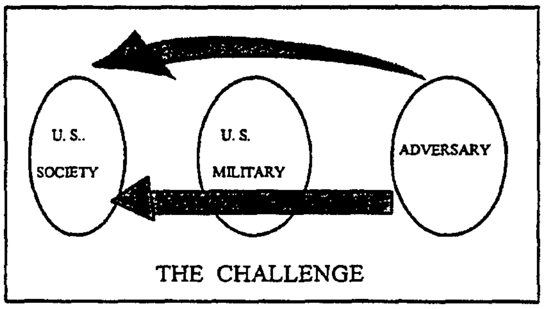


Figure 2. The Lost Sanctuary

The important consequence which the paradigm shift reveals is the opportunity Cyberspace provides to adversaries; a new dimension and approach for indirect or direct attacks on critical strengths, weaknesses, and vulnerabilities in our society. They are the new perimeter which must be defended if the enemy is to be defeated in his attempts to defeat our strategic center of gravity (COG). Our COG, which in the past may have required massive physical efforts to attack is now made vulnerable by the global connectivity of Cyberspace afforded by such systems as the "information superhighway."[6] It is therefore through Cyberspace, that a knowledgeable adversary may circumvent military force, and geography and exploit the once secure critical factors.[7]

Vulnerability Characteristics within the Lost Sanctuary

Attacks on critical factors via Cyberspace will provide unique and challenging situations. Attacks could be very economical for a knowledgeable adversary to make since a minimal investment in hardware is all that is required; "for the price of a $2,000 computer and a $200 modem you potentially can throw a multibillion dollar, high-tech military such as the United States' into chaos."[8] As an example, if the transportation and logistics information systems were targeted, the timely and complex movement of men and material could be hampered by computer induced "glitches." Material could be lost and manpower delayed. In today's conflicts, timely response could be the key difference between deterrence and escalation. Contrasting this with the massive effort demonstrated in the Pacific during WWII in cutting off Japan's LOC's reveals that a modern day adversary would not require a large Navy to interdict U.S. LOC's if it can disrupt the supplying sources for those LOC's. Such a capability demonstrates the leverage that information technology provides and certainly bolsters the idea of an adversary's economy of force.

Attacks will also be capable of being generated by anyone with little or no warning making it difficult in assessing strategic or even tactical situations for decision makers even as reaction time shrinks.[9] Operational surprise may be even easier to achieve. Information will be susceptible to tainting or compromise without the knowledge of the end user manifesting a new dimension in operational deception.[10] Because of the interconnectivity in Cyberspace, traditional boundaries and jurisdictions may become fogged. Such obscurity could lead to confusion as to who is under attack or who should respond.[11] Systems which interconnect or utilize products generated via Cyberspace such as C4I and high tech weapons, the new bastions of the U.S., are vulnerable. Since the vast information-sharing network leaves few clues as to where an attack originated from or who conducted an attack, knowledge of how present and future Cyberspace weapons operate as well as their methods of employment are the only means by which defenses can be made.

The Arsenal in Cyberspace

The array of weapons available for use in Cyberspace are numerous and complex. Some of the cyber weapons available are computer viruses; a subset of what is known in the computer world as "malicious codes."[12] Malicious codes come in different types and serve different functions which makes it important in understanding these codes. Viruses are characterized by being extremely efficient pieces of codes, often consisting of fewer than 100 bytes compiled. This simplicity of character and attack strategy is one of the reasons why computer viruses succeed. [13] They can be easily masked by the complexity of other computer programs, to which they become attached.

Worms are another subset of malicious codes and differ from viruses in one subtle but important way; a worm does not require a host [does not attach itself to a program]. "Whil virus can only be replicated by running an infected programme, a worm can take advantage of loopholes in an operating system applying a direct attack strategy."[14] As a worm self replicates, it can deny access to a system by overwhelming that system with its progeny.[15]

Trojan horses comprise a sinister subset of malicious codes since they are "designed to impersonate legitimate programmes."[16] Codes of this nature can allow for the theft of passwords in computer systems or the generation of surreptitious copies of data.

Logic bombs are usually improperly written legitimate code which were the result of faulty programming; the year 2000 problem for example. However, deliberate logic bombs such as a "trap door" may be used by unintended parties to bypass or shortcut security procedures."[17] Other types can be highly destructive and can lay dormant waiting for certain events to occur before destroying computer information.

A logic torpedo is a controlled virus which is aimed at one or more systems. Launched into Cyberspace, the logic torpedo tracks down its target (particular type of program) which it then infects.[18]

Time bombs are similar to logic bombs but are activated by a "specific time rather than a logic state."[19] A time weapon targets the internal clock of the computer which ultimately affects timing and synchronization leading to great difficulty in the system's ability to communicate.

Hybrid malicious codes produced by the "fusion" of viruses, worms, logic bombs, and trojan horses could be designed to "remain transparently dormant until a pre-determined time or series of events cue it to life. Once active, the virus may remain actively persistent or target a specific computer function before returning to its dormant state."[20]

Cyber weapons introduce challenging problems to the users of any computerized system. Most important of which are integrated computer network systems such as telecommunications, C^2, power grids, and air traffic control.[21] Because these systems share information, whether it is through the Internet or another information sharing provider, their openness makes them highly susceptible to electronic sabotage.[22] However, centralized information exchange systems are not the only targets. Computer virus warfare (CVW) "poses an interesting problem to manufacturers of advanced combat platforms where the trend is for increased reliance on software to operate many of the key sub-systems; such as sensors, command networks, and even flight controls."[23] Viruses in the form of logic bombs and trojan horses can be installed in software programs. "With the witting or unwitting cooperation of a software manufacturer, a "trap door" can easily be written into almost any commercial software application."[24] Trap doors, whether as software or hardware mechanisms, are often times added as a safety measure by a programmer or manufacturer to bypass a system hang up due to glitches in the program or its hardware. With this ability to use a back door to go around security features in the program, there is a means to fix bugs, no matter what the problem may be.

The arsenal to do battle in Cyberspace will also include radio frequency (RF) weapons. By the synchronous pulsing of electromagnetic energy at a specific frequency, digital signals (logic ones and zeroes) can be emulated. Utilizing this method would allow for the manipulation of data as well as the remote insertion of viruses.[25] Data manipulation is one area which will provide an attacker with a wide array of possibilities to exploit.

The age-old practice of utilizing spies will continue in Cyberspace due to the potential advantages which can be achieved. All facets of Cyberspace are vulnerable; including system network managers, software, and hardware production personnel bringing a new dimension to war. Compromised software and bobby-trapped computer chips could be inserted during the manufacturing process of weapons and C^2 systems. The compromised chips may not be identified until in a hostile situation;[26] in the heat of battle it will be too late to start swapping out computer chips, if the problem becomes apparent at all.

Employment of Weapons in Cyberspace

The contestants on the common ground of Cyberspace will employ a wide variety of methods. However, the basic goals of Cyberspace weapons will be the denial, destruction, and exploitation of information or any combination thereof.[27] Just as there is a wide spectrum of weapons which can be used, there are also many means to use them.

Viruses and logic weapons may be injected directly into a system or network. Known as a "direct launch," such a method may not discriminate and could lead to possible fratricide or collateral damage, requiring the protection of ones own COG.[28]

"Forward basing," like "direct launch" describes another method of introducing weapons into a system or network. The difference is that these weapons lie dormant, waiting for an event to take place or to be triggered or activated when required.[29] Such weapons could allow for operational sequencing by being part of a larger arrangement of events to attack an enemy's COG. By employing a barrage of these weapons into various targeted systems, operational synchronization could be achieved as the weapons worked in concert producing a synergistic effect. Operational phasing could also be achieved as one group of weapons achieved their objective which would then trigger another group of weapons into action.

Although DoD and Joint Publication 1-02 defines directed energy weapons as systems capable of destroying or damaging enemy equipment,[30] the use of directed energy, such as coherent RF signals, would provide for a non destructive method for "remote insertion" of "directed-energy viruses" into a system or network via an unprotected port such as a modem or power supply.[31]

"Hacking" is a well publicized method which utilizes the various cyber weapons to gain access, deny, exploit, or destroy a system. As early as 1994, unclassified documented cases of compromise to Department of Defense (DoD) computers were made known by the Government Accounting Office (GAO). The computer systems of the Air Development Center, the Air Forces's laboratory in Rome N.Y., where the DoD conducts some its research on weapons systems was accessed by two computer hackers. During the several days when access was gained, the intruders were able to gain complete access on all information including wartime methods used by Air Force commanders to relay secret intelligence and targeting information.[32] During this time, with complete access, the hackers could have installed a virus which could have done severe damage.[33] This same incident also revealed the vulnerability that the Internet has in networking with other computers and which is how many of the DoD's computers disseminate information including the possibility of computer viruses. During the same hacking incident, illegal access was made into "military, government, commercial, and academic systems worldwide" of which Wright-Patterson Air Force Base and Goddard Space Flight Center were just two of the systems that were compromised.[34] The occurrence of compromise of such systems, especially in DoD, is growing at a rapid rate. The GAO estimates that 250,000 hacker attacks occurred on DoD computers in 1995 and that figure will double every year.[35]

The Critical Factors

Operational art teaches that the identification of both enemy and friendly critical factors (critical strengths and critical weaknesses) is key to success in war. For by identifying the enemy's critical strengths, their destruction or neutralization will weaken the COG. Identifying the enemy's critical weaknesses can allow for further analysis in determining critical vulnerabilities if those weaknesses are associated with the COG [36] This analysis will also aid in determining where the sector of main effort will be focused and the decisive points to be achieved.

Cyberspace itself is at the same time a critical strength and a weakness. As a strength, it enhances all facets of the operational scheme. Various methods (cyber weapons employment) of defeating an opponent can be utilized through direct or indirect attacks on both tangible and intangible objectives via Cyberspace. Points of main attack are accessible through the application of cyber weapons. They can be used to carry out operational deception or for operational fires. The use of logic weapons allows for operational sequencing, synchronization, pause, and phasing.

As a weakness, the global connectivity of Cyberspace allows for reciprocative exploitation of unprotected U.S. critical factors. By providing an adversary the ability to reciprocate attacks, unprotected critical strengths and weaknesses operating through the utility of Cyberspace can become critical vulnerabilities. Cyberspace could be considered a critical vulnerability since it affords a globally accessible and unprotected medium for systems to network in. Unprotected critical strengths or weaknesses, that utilize an unprotected Cyberspace, can become critical vulnerabilities. " Sometimes critical strengths, such as C4I or excellent logistical support and sustainment, can become critical vulnerabilities. This is true if various elements of these capabilities are insufficiently protected and thereby potentially open to our attack."[37]

With the advantages that computers provide in determining supply requirements, tracking deliveries, and allocating requirements, computerized logistical systems in the U.S. are lucrative targets. Disrupting systems or networks which exchange such information could hamper successful employment of logistical support. During Desert Storm, about 98% of the logistics' information was processed through unclassified, commercial communications of which the least controllable was the Internet.[38] Although there has been no "creditable method" to cause a complete shut down of the Internet, the possibility looms. Until such time that it happens, the Internet remains as a viable and effective "auxiliary" to a military network that could be easily compromised in war or peace.[39] For the military logistician, the ability to enhance logistics information exchange will be accomplished through the Global Transportation Network (GTN). But even this new system, which fuses transportation information from numerous sources including commercial carriers and shippers, may be susceptible to attack since it will utilize public switched telephone networks in part of the information exchange scheme.[40] Due to the highly developed infrastructure within the U.S. , this critical strength can be highly vulnerable to attack if not adequately protected.

Modern, computerized industrial bases open up a whole new realm of potential critical strengths and weaknesses to attack via Cyberspace. Production lines, R&D efforts, and employment driven by computers are all vulnerable.[41] By inducing errors in the R&D efforts in a system's development, a country could be denied the use of the new capability. Confidence in developing such technology might even wane thereby keeping it from exploring other innovative methods. Such infrastructures are vulnerable to "forward basing" of agents as well as "remote strikes" by hackers.

U.S. C^2 infrastructures including those which support transportation such as rail systems and civil aviation are critical strengths. The complex network which synchronizes their movement is vulnerable to compromise. Undermining their safety and reliability would ultimately undermine the confidence of the public which depends on these systems for transportation. C^2 vulnerabilities also include a nation's "civilian and strategic leadership, the decision process, societal support structures such as the police, and other governmental entities like the Bureau of Land Management and the strategic oil reserves. Attacking these targets can sow discord in an opponent's society, thereby fracturing the decision-making process or any consensus; deny an opponent the ability to marshal needed resources to rebuff an attack; or divert attention from other activities."[42] With the deleterious effect on the national will, this critical strength also becomes a COG. With the development of GCCS, the military will have a secure (encrypted) method to exchange information up to the highest levels of decision makers (NCA).[43] Consequently, it will be the unprotected C^2 system in the civilian sector which could gravitate to become a critical vulnerability and a possible COG.

Utilities such as electrical power plants and phone service providers in the U.S. which rely on networked computers to manage and distribute the flow of power and relay phone calls are critical strengths. However, with an interface into Cyberspace, power plants which feed into a power grid are susceptible to the targeting of their control systems which allow for the distribution of power. Creating power sinks by draining power out of the grid could lead to massive brown-and blackouts.[44] A massive loss of phone service could induce chaos, especially if it were coupled with a severe power loss. Consequently, such systems if operating unprotected can become critical vulnerabilities.

The critical strength of the U.S. economic sector provides myriad possibilities for attack via Cyberspace. Computers are infused into the control mechanisms of debt, tariffs, price controls, and exchange rates.[45] Banks and other financial institutions rely on automated methods to transfer money. ATMs are a mainstay in the U.S. Rand Corporation's wargame, "The Day After...in Cyberspace," which was played by senior U.S. officials revealed key items to exploit in bringing a nation to the bargaining table during future conflicts: degradation of computer controlled assets such as satellite surveillance, communications, commercial aviation, banking, and information exchange systems in business were pivotal in producing victory in the age of information war.[46] Attacks on these "selected nodes of American social and economic fabric..." would produce strategic results.[47] Confidence would wane in the economy as the data bases for financial markets, stock exchanges and banking systems were manipulated to produce deleterious interest rates, substandard profits, and losses to savings. Targets could be prepped months or years in advance and subtly attacked. The strategic repercussions alone provides the impetus for any knowledgeable adversary: terrorist, guerrilla, or rogue nation, to employ a focused effort in compromising these systems.[48] Unprotected, this critical strength could become a critical vulnerability and a possible COG.

The critical strength of U.S. public transportation, which has come to depend on computers to make travel efficient, is also susceptible to exploitation. The psychological effect of removing the efficiency, dependability, and potential of such a system could induce "cascading chaos"; hampering efficient transportation means a society may be without the basics for sustenance, or weapons and fuel to carry on a war could be diverted or lost in a massive and complex transportation infrastructure. [49]

Military training becomes an exploitable intangible critical strength if a nation fights as it trains. By manipulating statistics and data bases or by incorporating tainted information into a resulting training scheme, a compromised system of training could be generated. One method of subversion would be for an adversary to "leak" an altered training manual to the nation which it had planned to attack.[50] Lack of training in computer systems security is a critical weakness which the Defense Information Systems Agency (DISA) has been grappling with since 1992 when it developed "Red Teams" to attack friendly computer networks in order to assess vulnerability. Since that time, 38,000 attacks were initiated with 65% having breached the computers with the disheartening fact that only four percent of attacks were recognized by system administrators.[51]

Critical Vulnerabilities:

With the proliferation of information age hardware and software and the ever-shrinking technology life cycle, DoD has shifted from "being the driving force in information technology to being a specialty user...."[52] Austere budgets have forced the DoD to forego development of specialty high technology systems and rely on commercial-off-the-shelf (COTS) technology to allow for timely acquisition and in order to "field cost-effective systems."[53] In addition, there are "aging systems" that need replacement to ensure that continued readiness is maintained.[54]

COTS technology inherits vulnerabilities some of which computer viruses can exploit. Military systems will now be based on systems architectures and components which are available to any potential adversary to systematically investigate. They can produce tailored computer viruses to target the associated hardware and supporting software. Captured military equipment, especially highly developed and non-COTS technology, is also susceptible to hardware and software compromise. A determined adversary can reverse engineer a system and develop computer viruses to be used immediately or in the future. The nature of the virus could be to cause complete failure of a system or to inject tainted information. The latter will produce uncertainty in the quality of information and tax decision makers at all levels of command and control. Such a vulnerability will require "unique keys that identify and authorize users on particular systems, devices that report current locations on key hardware items via satellite, authentication procedures, and security codes" to combat the exploitation of such systems.[55]

In the defense sector, where computer software has provided the enhanced capabilities for equipment and systems, the vulnerabilities are just as ominous.[56] Software has basically "touched" every piece of military hardware, and since "no software is completely testable because of the large number of possible execution paths...",[57] the threat of compromised systems could certainly be diverse and substantial. But what characterizes such risk is the fact that tampered software can be an insidious threat. In affected systems, the normal external operation of that system may in fact belie an embedded weakness only to be revealed when it is too late to do anything about it.

Protection in Cyberspace

The common link that is shared by the computer dependent critical factors is the information infrastructure and associated connectivity which make up Cyberspace. One method in protecting the information exchange has been through encryption. However, due to incompatibility and standardization, establishing an encryption system capable of communicating on a network with foreign allies and especially within a diverse civilian sector is a problem.[58] For the U.S. military, systems such as GCCS will provide the protection and security required to exchange sensitive information. But this does not solve the problem for the previously sanctuaried critical factors. Although encryption can make it much more difficult for an adversary to compromise a system, risks still remain. As long as there is an electronic link (computer interconnectivity) or a medium to utilize directed energy weapons, critical strengths and weaknesses are susceptible to destruction, denial, or compromise. In the civilian sector, where encryption methods are utilized in but a few of the economic sectors, operational security will have to rely on awareness. The key to improved security in the short term is increased awareness of the potential damage network breaches can cause.[59]

Conclusion

In 1996, DoD had over "2.1 million computers, 200 command centers, 16 central computing "MegaCenters," 10,000 local networks and 100 long-distance networks,...."[60] Coupled with the trend for increased utilization of COTS and software enhanced systems, the increased push to employ the utility of Cyberspace brings with it an exponential increase in vulnerabilities to economic, military, social, and political critical factors. The lever arm of technology and its offspring; cyber weapons, will expose the sanctuaried critical factors. "The implications of warfare in the information arena are enormous. First, national homelands are not sanctuaries. They can be attacked directly, and potentially anonymously, by foreign powers, criminal organizations, or non-national actors such as ethnic groups, renegade corporations, or zealots of almost any persuasion. Traditional military weapons cannot be interposed between the information warfare threat and society."[61]

Encryption methods and operational security training will afford some protection, but incompatibility between the vast types of networked systems and the continually shrinking technology life cycle in both sectors will remain a problem as distinctions between military and non-military systems become hard to differentiate. The National Security Agency estimates that there are more than 120 nations that have established "information warfare cadres" which are designed to take advantage of an adversary's weaknesses in operational security.[62] The return on the investment in a simple computer system equipped with a modem provides the potential to effect multi-billion dollar damage on a high tech military.

U.S. planners, especially at the strategic and operational levels, must appreciate the complexity in planning for defenses and protection of U.S. critical factors; for with the new opportunities in Cyberspace come vulnerabilities. Strategic geography and military force has been made transparent by the global connectivity afforded by Cyberspace.

Notes

[1] David S. Alberts, *The Unintended Consequences of Information Age Technologies* (Washington, D.C.: National Defense Univ., 1996), 27.

[2] Steve Lambert and Walt Howe, *Internet Basics* (New York: Random House 1993), 459.

[3] Office of the Joint Chiefs of Staff, *Joint Command and Control, Communications, and Computers Systems Descriptions Volume I* (Washington D.C.: 1994), 84.

[4] Mark Mateski, "Beyond Metaphors: Information Warfare and Systems Thinking," *Jane's US Information Warfare E-Letter*, 27 January 1997, 1.

[5] *The Littoral and Information Warfare Conference*, unpublished conference presentation notes, U.S. Naval War College, Newport, R.I.: 3 March 1995, III-6.

[6] Stephen M. Hardy, "Should We Fear the Byte Bomb?," *Journal of Electronic Defense*, January 1996, 45.

[7] Ibid.

[8] Stephen M. Hardy, "The New Guerrilla Warfare." *Journal of Electronic Defense*, September 1996, 50.

[9] Hardy, "Should We Fear the Byte Bomb?," 45.

[10] Ibid., 45.

[11] Mark Thompson, "If War Comes Home," *Time*, 21 August 1995, 46.

[12] Mark Bently and Paul Evancoe, "CVW - Computer Virus as a Weapon," *Military Technology*, May 1994, 38.

[13] Ibid.

[14] Ibid., 39.

[15] Center for Naval Analyses, *Offensive Information Warfare--A Concept Exploration.* (CIM 361. Alexandria: VA. 1994.) 17.

[16] Bently and Evancoe, 39.

[17] Ibid.

[18] Center for Naval Analyses, 6.

[19] Ibid.

[20] Bently and Evancoe, 39.

[21] Hardy, "Should We Fear the Byte Bomb?," 45.

[22] Michael Howard and John F. Guilmartin, Jr. *Two Historians in Technology and War* (Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA. July 1994.) 33.

[23] Bently and Evancoe, 40.

[24] Center for Naval Analyses, 6.

[25] Ibid.

[26] Douglas Waller, "Onward Cyber Soldiers," *Time*, 21 August 1995, 41.

[27] Center for Naval Analyses, 10.

[28] Ibid.

[29] Ibid.

[30] Office of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, D.C.: 1984) 117.

[31] Center for Naval Analyses, 10.

[32] Philip Shenon, "Report Warns of Security Threats Posed by Computer Hackers," *The New York Times*, 23 May 1996, A22:1.

[33] Howard and Guilmartin, 33.

[34] Shenon, A22:1-2.

[35] John J. Fialka, "Pentagon Hacker Attacks Increase And Some Pose Threat, GAO Says," *The Wall Street Journal*, 23 May 1996, B3:1.

[36] Milan N. Vego, "Elements of Operational Warfare," NWC 4096, unpublished paper, U.S. Naval War College, Newport, R.I.: August 1996, 3.

[37] Ibid.

[38] Hardy, "The New Guerrilla Warfare," 48.

[39] Ibid., 50.

[40] *Joint Command and Control, Communications, and Computers Systems Descriptions Volume I*, 89.

[41] Center for Naval Analyses, 12.
[42] Ibid.
[43] *Joint Command and Control, Communications, and Computers Systems Descriptions Volume I*, 84.
[44] Center for Naval Analyses, 13.
[45] Ibid., 12.
[46] Thompson, 45-46.
[47] Howard and Guilmartin, 34.
[48] Richard O. Hundley and Robert H. Andersen, *Security In Cyberspace: An Emerging Challenge For Society*, RAND, P-7893, 1994, 6.
[49] Center for Naval Analyses, 14.
[50] Ibid.
[51] Hardy, "The New Guerrilla Warfare," 48.
[52] Alberts, 27.
[53] Ibid.
[54] "Commercial Information Systems Proliferate in Military Operations," *Signal*, January 1997, 63.
[55] Alberts, 41.
[56] Peter Emmett, "Information Mania-A New Manifestation of Gulf War Syndrome?" *RUSI Journal*, February 1996, 23.
[57] Ibid.
[58] Hardy, "The New Guerrilla Warfare," 52.
[59] Hundley and Andersen, 49.
[60] Hardy, "The New Guerrilla Warfare," 48.
[61] Alberts, 27.
[62] Hardy, "The New Guerrilla Warfare," 50.

Bibliography

Alberts, David S. *The Unintended Consequences of Information Age Technologies*. Washington, D.C.: National Defense Univ., 1996.

Bently, Mark and Paul Evancoe. "CVW - Computer Virus as a Weapon." *Military Technology*, May 1994, 38-40.

Center for Naval Analyses. *Offensive Information Warfare--A Concept Exploration.* CIM 361. Alexandria, VA: 1994.

"Commercial Information Systems Proliferate in Military Operations." *Signal*, January 1997, 63-65.

DOD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985.

Emmett, Peter. "Information Mania-A New Manifestation of Gulf War Syndrome?" *RUSI Journal*, February 1996, 19-26.

Fialka, John J. "Pentagon Hacker Attacks Increase And Some Pose Threat, GAO Says." *The Wall Street Journal*, 23 May 1996, p. B3:1-2.

Hardy, Stephen M. "Should We Fear the Byte Bomb?." *Journal of Electronic Defense*, January 1996, 42-47.

________. "The New Guerrilla Warfare." *Journal of Electronic Defense*, September 1996, 46-62.

Howard, Michael and John F. Guilmartin, Jr. *Two Historians in Technology and War*. Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA. July 1994.

Hundley, Richard O. and Robert H. Andersen. *Security In Cyberspace: An Emerging Challenge For Society.* RAND, P-7893, 1994.

Lambert, Steve and Walt Howe. *Internet Basics*. New York: Random House, 1993.

Mateski, Mark. "Beyond Metaphors: Information Warfare and Systems Thinking," *Jane's US Information Warfare E-Letter*, 27 January 1997.

Office of the Joint Chiefs of Staff, *Joint Command and Control, Communications, and Computers Systems Descriptions Volume I* (Washington D.C.: 1994)

Office of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, D.C.: 1984)

Shenon, Philip. "Report Warns of Security Threats Posed by Computer Hackers." *The New York Times*, 23 May 1996, p. A22:1-6.

The Littoral and Information Warfare Conference, unpublished conference presentation notes, U.S. Naval War College, Newport, R.I.: 3 March 1995.

Thompson, Mark. "If War Comes Home." *Time*, 21 August 1995, 44-46.

Waller, Douglas. "Onward Cyber Soldiers." *Time*, 21 August 1995, 38-44.

Additional Reading

Barnaby, Frank and Marlies ter Borg. ed.,*Emerging Technology and Military Doctrine*. New York: St. Martins Press Inc, 1986.

Blackwell, James and Anthony H. Cordesman, *Strategy and Technology*. Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA. April 1992.

Emmett, Peter. "Software Warfare: The Militarization of Logic," *Joint Forces Quarterly*, Summer 1994; 84-90.

Jeremiah, Adm, David E. "How Rapid Technological Change Will Change Warfare." *Asia-Pacific Defence Reporter*, October-November 1993, 26-27.

Libicki, Martin C. *What is Information Warfare?* Washington, D.C.: National Defense Univ., 1995.

"Panel to Oversee Protecting Systems From Hackers." *The Wall Street Journal*, 17 July 1996, p. B8:1.

Shukman, David. *Tomorrow's War The Threat of High-Technology Weapons*, New York: Harcourt Brace, 1996.

Weiner, Tim. "Head of C.I.A. Plans Center To Protect Federal Computers." *The New York Times*, 26 June 1996, p. B7:5.

Electronic References

Internet Locations

Note: The following URLs are current as of the date of publication

General:

Bibliography of Information Warfare and Infrastructure Vulnerability Documents
http://www.aracnet.com/~gtr/archive/info_war.html#dsb

Information Warfare sites
http://www.webcom.com/~amraam/othiw.html

Sanz, T.
"Information-Age Warfare: A Working Bibliography"
http://www-cgsc.army.mil/milrev/English/MarApr98/sanz.htm

Books & Articles:

Alberts, D.S.
"The Unintended Consequences of Information Age Technologies"
National Defense University Press, April 1996
http://www.ndu.edu/ndu/inss/books/uc/uchome.html

Alberts, D. S.
"Defensive Information Warfare"
National Defense University, Press, Aug 1996
http://www.ndu.edu/ndu/inss/books/diw/index.html

Anderson, Kent E.
"Intelligence-Based Threat Assessments for Information
Networks and Infrastructures: A White Paper"
Global Technology Research Inc., March 11, 1998
http://www.aracnet.com/~kea/Papers/threat_white_paper.shtml

Arquilla, John and Ronfeldt, David
"In Athena's Camp: Preparing for Conflict in the Information Age"
MR-880-OSD/RC Rand Corp., 1997
http://www.rand.org/publications/MR/MR880/contents.html

Bowers, S.R.
"Information Warfare: The Computer Revolution is Altering How Future
Wars Will be Conducted"
Armed Forces Journal International, 136:38-39, August 1998
http://www.afji.com/mags/1998/august/information%20warfare/index.html

Browning, G.
"Infowar"
GovExec. Com, April 21, 1997
http://www.govexec.com/dailyfed/0497/042297b1.htm

Correll, John T.
"War in Cyberspace",
Air Force Magazine, 81:32-36, January 1998
http://www.afa.org/magazine/0198warin.html

Report of the Defense Science Board Task Force on Information Warfare
Defense IW-D, November 1996
http://cryptome.org/iwd.htm

Devost, M.G., Houghton, B.K., and Pollard, N.A.
"Information Terrorism: Can You Trust Your Toaster?" Sun Tzu Art of War Information Warfare Compendium, Institute for National Strategic Studies, National Defense University, 1997
http://www.ndu.edu/inss/siws/ch3.html

General Accounting Office (GAO), "GAO Executive Report - B-266140", Report to the Committee on Governmental Affairs, U.S. Senate, May 22, 1996
http://epic.org/security/GAO_DOD_security.html

General Accounting Office (GAO), "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks", (Chapter Report, 05/22/96, GAO/AIMD-96-84)
http://www.us.net/softwar/gao.html

Harley, J.A.
"Information Technology and the Center of Gravity"
Naval War College Review, Winter 1997
http://www.nwc.navy.mil/press/Review/1997/winter/art4wi97.htm

Kluepfel, H.
"Countering Non-lethal Information Warfare", Proceedings of the IEEE 29th Annual International Carnahan Conference on Security Technology, 1995
http://www.infowar.com/CIVIL_DE/kluepfel.html-ssi

Koprowski, G.
"Hacking the Power Grid"
Wired News, June 4, 1998
http://www.wired.com/news/news/technology/story/12746.html

Overbeck, C.
"Pentagon CyberTroops: The National Security Apparatus
Gears Up for Infowar"
Parascope, 1997
http://www.parascope.com/articles/0297/infowar.htm

ADDITIONAL REFERENCES

Note: refer to the order form following the bibliographies for ordering information.

AD-A372229

OBJECT SERVICES AND CONSULTING INC
BALTIMORE MD

Survivability in Object Service Architectures (OSA)

OCT 1999 167 PAGES

PERSONAL AUTHORS: Wells, David; Ford, Steve; Langworthy, David; Bannon, Thomas; Wells, Nancy

UNCLASSIFIED REPORT

ABSTRACT: (U) The military of the future will increasingly rely upon information superiority to dominate the battlespace. This report summarizes the goals and results of a project that developed an architecture and software mechanisms to make military and commercial software applications based on the popular object services architecture (e.g., OMG's CORBA) model far more survivable than is currently possible, while at the same time maintaining the flexibility and ease of construction that characterizes OSA based applications.

DESCRIPTORS: *DISTRIBUTED DATA PROCESSING, *TACTICAL DATA SYSTEMS, *NETWORK ARCHITECTURE, DATA PROCESSING SECURITY, MILITARY APPLICATIONS, COMPUTER PROGRAM VERIFICATION, OBJECT ORIENTED PROGRAMMING, INFORMATION WARFARE, RISK ANALYSIS.

AD-A371775

NAVAL POSTGRADUATE SCHOOL
MONTEREY CA

Summary of Research 1998, Interdisciplinary Academic Groups

AUG 1999 121 PAGES

PERSONAL AUTHORS: Boger, Dan; Powell, James; Panholzer, Rudolf; Eagle, James

UNCLASSIFIED REPORT

ABSTRACT: (U) This report contains information of research projects in the interdisciplinary: (1) groups, command, control, and communications academic group, (2) information systems academic group, (3) information warfare academic group, (4) space systems academic group, and (5) undersea warfare academic group. A list of recent publications is also included which consists of conference presentations and publications, books, contributions to books, published journal papers, technical reports, and thesis abstracts.

DESCRIPTORS: *COMMAND CONTROL COMMUNICATIONS, *SPACE SYSTEMS, *UNDERSEA WARFARE, *INFORMATION WARFARE, SOFTWARE ENGINEERING, STRATEGIC ANALYSIS, COMPUTER NETWORKS, RADAR SIGNALS, RESEARCH MANAGEMENT, THEATER MISSILE DEFENSE, COMBAT SIMULATION.

AD-A371754

ELECTRONICS RESEARCH LAB
SALISBURY (AUSTRALIA)

Achieving Systemic Information Operations for Australian Defence

OCT 1999 28 PAGES

PERSONAL AUTHORS: Staker, R. J.

UNCLASSIFIED REPORT

ABSTRACT: (U) This document describes a proposed program of research into theories, methodologies and techniques appropriate to achieving a systemic military information operations capability for the Australian Defence Force. The major expected outcomes of this research are decision support aids relevant to information operations, contributions to the theory of information operations and contributions to IO policy and doctrine. The doctrine would include matters relating to the design of organisations that are capable of operating effectively in an information operations environment.

DESCRIPTORS: *MILITARY INTELLIGENCE, *COMMAND AND CONTROL SYSTEMS, *AUSTRALIA, *INFORMATION WARFARE, MILITARY FORCES (FOREIGN), MILITARY DOCTRINE, HUMAN FACTORS ENGINEERING, MILITARY CAPABILITIES, DECISION AIDS, DECISION SUPPORT SYSTEMS.

AD-A370937

STATE UNIV OF NEW YORK AT BUFFALO
CENTER OF MULTISOURCE
INFORMATION FUSION

Studies and Analyses of Aided Adversarial Decision Making. Phase 2: Research on Human Trust in Automation

APR 1998 119 PAGES

UNCLASSIFIED REPORT

PERSONAL AUTHORS: Llinas, James; Bisantz, Ann; Drury, Colin; Seong, Younho; Jian, Jiun-Yin

ABSTRACT: (U) This report describes the second phase of work conducted at the Center for Multi-Source Information Fusion at the State University of New York at Buffalo. This work focused on Aided Adversarial Decision Making (AADM) in Information Warfare (IW) Environments. Previous work examined informational dependencies and vulnerabilities in AADM to offensive IW operations. In particular, human trust in automated, information warfare environments was identified as a factor which may contribute to these vulnerabilities and dependencies. Given that offensive IW operations may interfere with automated, data-fusion based decision aids, it is necessary to understand how personnel may rely on or trust these aids when appropriate (e.g., when the information provided by the aids is sound), and recognize the need to seek other information (i.e., to "distrust' the aid) when the information system has been attacked. To address these questions, this report details background research in the areas of human trust in automated systems and sociological findings on human trust, details the development of an empirically-based scale to measure trust, provides a framework for investigating issues of human trust and its effect on performance in an AADM-IW environment, and describes the requirements for a laboratory designed to conduct these investigations.

DESCRIPTORS: *DECISION MAKING, *PERFORMANCE (HUMAN), AUTOMATION, INFORMATION SYSTEMS, HUMAN FACTORS ENGINEERING, DATA FUSION, DECISION AIDS, INFORMATION WARFARE.

AD-A370865

NAVAL WAR COLL NEWPORT RI

Intermediate Operational Commanders. A Role for Naval Destroyer Squadron Commanders

17 MAY 1999 22 PAGES

PERSONAL AUTHORS: Sweeney, Michael J.

UNCLASSIFIED REPORT

ABSTRACT: (U) Advances in Information Technology (IT) Systems and Decision Aids offer increased speed of command in warfare. What effect does it have on the authority of intermediate operational commanders such as Destroyer Squadron (Desron) commanders in the U. S. Navy? Intermediate commanders remain vital to manage the "how" to complete the operational scheme of Joint Force Commanders (JFC) despite the increased availability of shared information. Desron commanders traditional and current roles offer leadership experience to provide intuitive decision making and prepare the battlefield in maritime service applications and joint operations.

DESCRIPTORS: *MILITARY MODERNIZATION, *DECISION AIDS, *INFORMATION WARFARE, NAVAL PERSONNEL, THESES, NAVAL VESSELS (COMBATANT), MILITARY CRITICAL TECHNOLOGY.

AD-A370751

NAVAL WAR COLL NEWPORT RI

Net-Centric Warfare: Are We Ready to be Cyber-Warriors?

17 MAY 1999 21 PAGES

PERSONAL AUTHORS: Monroe, Deborah

UNCLASSIFIED REPORT

ABSTRACT: (U) Joint Vision 2010, the chairman of the Joint Chiefs of Staff's template for future military operations, identifies information superiority as the linchpin of the emerging operational concepts of dominant maneuver, precision engagement, focused logistics and full dimensional protection. While the technical challenges to realizing these concepts are acknowledged, I contend the tasks required to successfully integrate the human and cultural side of Joint Vision 2010's information superiority are as daunting as any of the still unsolved technical hurdles. Currently, the human element of technology enabled warfare is not getting the attention it needs. The military must begin to examine whether current training and doctrine are sufficient to prepare operational commanders for the chairman's vision of the future.

DESCRIPTORS: *COMBAT READINESS, *MILITARY PLANNING, *INFORMATION WARFARE, MILITARY REQUIREMENTS, MILITARY DOCTRINE, MILITARY CAPABILITIES, JOINT MILITARY ACTIVITIES, MANEUVERS.

AD-A370707

NAVAL WAR COLL NEWPORT RI
JOINT MILITARY OPERATIONS DEPT

Warfare in the Information Age: Adding Capability Multipliers

17 MAY 1999 25 PAGES

PERSONAL AUTHORS: Cooney, David M., Jr

UNCLASSIFIED REPORT

ABSTRACT: (U) One recurring theme in military writings since the end of Desert Storm is that the American military is on the cusp of a new revolution in military affairs (RMA). Proponents of this viewpoint cite major changes in business and society brought on by the personal computer and the internet. They view these changes as part of a new information age and predict that the explosive technological growth in the speed of microprocessors and networks will lead to whole new ways to wage war, with information superiority being the key ingredient to assure victory. Critics argue that war as a rough, brutish, and frequently irrational business, and that no network will eliminate either the fog or friction of war. They see many of concepts being put forward as not respectful of the enduring principles of war. This paper presents five capability multipliers for warfare in the information age: (1) assembling and maintaining the intellectual capital to operate in the future networks; (2) developing information as a true discipline; (3) improving human computer interaction; (4) seeking greater understanding of how people process information and make decisions; and (5) furthering the cultural, organizational and operational concepts to support the technological change.

DESCRIPTORS: *MILITARY OPERATIONS, IRAQ, KUWAIT, MILITARY REQUIREMENTS, INFORMATION EXCHANGE, MICROPROCESSORS, MILITARY CAPABILITIES, JOINT MICROCOMPUTERS, COMPUTER NETWORKS, MILITARY MODERNIZATION, INFORMATION WARFARE, SITUATIONAL AWARENESS.

AD-A370700

NAVAL WAR COLL NEWPORT RI

Will Network-Centric Warfare be the Death Knell for Allied/Coalition Operations?

17 MAY 1999 25 PAGES

PERSONAL AUTHORS: Geraghty, Barbara A.

UNCLASSIFIED REPORT

ABSTRACT: (U) The U.S. Navy is undergoing a shift in its focus from platform-centric to network-centric warfare in the coming century. Enabled by the recent advances in information technology, network-centric warfare connects widely dispersed platforms into a robust network capable of massing tremendous effects. Network-centric warfare will challenge the operational commander when planning allied/coalition operations in two major areas. The first is interoperability, which includes issues of technology compatibility, intelligence sharing, classified material security policy, language, and rules of engagement. The second challenge addresses the issue of command and control, specifically as national culture and subordination of forces affect it. The operational commander must determine the ability of coalition partner forces to be part of the network and assign mission tasks accordingly. As history has shown, coalition operations require significant leadership on the part of the commander and network- centric warfare is simply another factor to add to the challenge.

DESCRIPTORS: *MILITARY OPERATIONS, *COMMAND AND CONTROL SYSTEMS, POLICIES, INFORMATION EXCHANGE, INTEROPERABILITY, SECURITY, MILITARY CAPABILITIES, COMPUTER NETWORKS, MILITARY TACTICS, BATTLE MANAGEMENT, INFORMATION WARFARE.

AD-A370694

NAVAL WAR COLL NEWPORT RI

Network Centric Coalitions: Pull, Pass, or Plug-In?

15 MAY 1999 25 PAGES

PERSONAL AUTHORS: Carr, James

UNCLASSIFIED REPORT

ABSTRACT: (U) The author traces the evolution of network centric warfare, showing its American roots. He shows that NCW is not a remote concept on the horizon, it is nascent in today's maritime operations and inevitably will be the way in which the U.S. Navy will fight future wars. Then he reveals a gaping mismatch between the emerging operational doctrine and the strategy it will be tasked to support. Since it is largely an American conception for warfare, the United States thus bears the burden to pursue interoperability with regional coalition partners if it is to fight "together when we can, alone if we must." Finally, the author presents options for addressing this strategic/operational mismatch and proposes a way ahead.

DESCRIPTORS: *WARFARE, *MILITARY STRATEGY, *INTEROPERABILITY, *NAVAL OPERATIONS, GLOBAL, UNITED STATES, OPERATIONAL EFFECTIVENESS, JOINT MILITARY ACTIVITIES, DOCTRINE, INFORMATION WARFARE.

AD-A370688

NAVAL WAR COLL NEWPORT RI

Information Warfare: Measures of Effectiveness

17 MAY 1999 23 PAGES

PERSONAL AUTHORS: Wright, Beverly C.

UNCLASSIFIED REPORT

ABSTRACT: (U) Information Warfare (IW) has become central to the way nations fight wars and technological advances on the horizon will only increase the importance of IW to the operational commander. The growing significance of IW requires the development of measures for determining its effectiveness. This paper specifically explores measures of effectiveness for C2-attack. Measuring the effectiveness of C2-attack actions is critical to the operational commander because effective C2-attack allows a commander to gain the initiative, thereby establishing and maintaining a primary advantage over an adversary. Since it is important to align measures of effectiveness with mission objectives or goals, possible measures of effectiveness are developed for each of the four goals of C2-attack. Developing meaningful measures of effectiveness for C2-attack is quite a challenge due to its significant subjective content. The dilemma is how to combine objective and subjective measures so the commander has a complete picture. In many respects, objective measures can be rolled up into an overall subjective measure. Some measures, however, just don't quantify well. As a commander plans a specific action and then implements that action, it is imperative he be able to measure the effectiveness of that action, analyze the results of that measurement, and then finally use the results of that analysis to plan the next action. Mastering this process may very well be one of the greatest challenges of command.

DESCRIPTORS: *INFORMATION WARFARE, COMMAND CONTROL COMMUNICATIONS, CONTROL, MEASUREMENT, ATTACK, COMMAND AND CONTROL SYSTEMS, TECHNOLOGY ASSESSMENT.

AD-A370329

ARMY COMMAND AND GENERAL STAFF COLL FORT LEAVENWORTH KS SCHOOL OF ADVANCED MILITARY STUDIES

Army Information Centers of Gravity: Can We Protect Them

27 MAY 1999 62 PAGES

PERSONAL AUTHORS: Carter, Rosemary M.

UNCLASSIFIED REPORT

ABSTRACT: (U) As the Army keeps pace with the information age, it must determine how to leverage information to win its wars. According to Brigadier General Wayne M. Hall information is a tool for influencing an enemy's decision cycles. This is achieved by attacking the enemy's information centers of gravity. BG Hall defines these information centers of gravity as the physical place or mental construct in cyberspace where a confluence of intellect, decisions, collection, automation, communications and planning occurs. The purpose of this monograph is to determine if the U.S. Army has information centers of gravity, and if so, can they be protected. The monograph first determined the key components of information from the definition of information superiority. These key components were analyzed using three criteria to determine the Army's information centers of gravity. The criteria used were their influence on decision cycles, effects on strategic aims, and impact on combat power. The analysis concluded that there are two information centers of gravity Army commanders and information operations cells. The monograph used the Army's defensive IO capabilities to determine if it can protect these information centers of gravity. The conclusion is that the U.S. Army does have the capability to provide protection for these information centers of gravity. The monograph concluded with a look at additional initiatives that are ongoing to protect both information centers of gravity and the key components of information that support these centers.

DESCRIPTORS: *COMBAT READINESS, *ARMY PLANNING, *INFORMATION WARFARE, MILITARY STRATEGY, DECISION MAKING.

AD-A369776

NAVAL POSTGRADUATE SCHOOL MONTEREY CA

Public Key Infrastructure (PKI) Interoperability: A Security Services Approach to Support Transfer of Trust

SEP 1999 167 PAGES

PERSONAL AUTHORS: Hansen, Anthony P.

UNCLASSIFIED REPORT

ABSTRACT: (U) Public Key Infrastructure (PKI) technology is at a primitive stage characterized by deployment of PKIs that are engineered to support the provision of security services within individual enterprises, and are not able to support the vendor-neutral interoperability necessary for large, heterogeneous organizations such as the United States Federal Government. Current efforts to realize interoperability focus on technical compatibility between PKIs. This thesis defines interoperability as the capacity to support trust through retention of security services across PKI domains at a defined level of assurance and examines the elements of PKI interoperability using this more comprehensive approach. The initial sections discuss the security services PKIs support, the cryptography PKIs employ, the certificate/key management functions PKIs perform, and the architectural elements PKIs require. This provides the framework necessary for discussing interoperability. Next, the two fundamental aspects of interoperability, technical and functional, are presented as well as their constituent elements and the existing barriers to interoperability. Finally, the proposed U.S. Department of Defense and Federal Government PKI architectures are analyzed and recommendations made to facilitate interoperability.

DESCRIPTORS: *CRYPTOGRAPHY, *DATA PROCESSING SECURITY, *COMPUTER COMMUNICATIONS, INFORMATION TRANSFER, INTEROPERABILITY, THESES, ONLINE SYSTEMS, COMPUTER PROGRAM VERIFICATION, INFRASTRUCTURE, INFORMATION WARFARE.

AD-A369372

ARMY SCIENCE BOARD
WASHINGTON DC

Concepts and Technologies for the Army Beyond 2010

MAR 1999 236 PAGES

PERSONAL AUTHORS: Braddock, Joseph V.; Funk, Paul E.; Gorman, Paul F.; Brady, Edward C.; Brown, William P.

UNCLASSIFIED REPORT

ABSTRACT: (U) A study assessing the 2010-2025 timeframe and seeking technologies and enablers for joint, Army and other service operations with emphasis on joint missions involving land combat. Specific areas of analysis include mobility and sustainment, information dominance, platforms and weapons and investment strategies. Study analyses suggest tapping commercial successes as private sector investment is strongly supporting improvements in many areas. However, to fully tap these developments the Army must begin participating in the design of future commercial systems. This study provides 9 major recommendations including: establishing an investment council, exploiting non-Army commercial capabilities, establishing a C4ISR testbed, and using FSCS vehicles as precursors for AA2010 platforms.

DESCRIPTORS: *ARMY PLANNING, *TECHNOLOGY FORECASTING, WEAPONS, LAND WARFARE, STRATEGY, INVESTMENTS, MISSIONS, COMMERCIAL EQUIPMENT, HOMING, INFORMATION WARFARE.

AD-A368431

NATIONAL DEFENSE UNIV
WASHINGTON DC INST FOR
NATIONAL STRATEGIC STUDIES

Defending Cyberspace and Other Metaphors

FEB 1997 113 PAGES

PERSONAL AUTHORS: Libicki, Martin C.

UNCLASSIFIED REPORT

ABSTRACT: (U) Information warfare, as any casual observer of the Pentagon can attest, remains a hot-button topic in the military community. Broader claims for it have been toned down, and few now argue that all aspects of warfare are now revealed as information warfare, but an ideology of information warfare has nevertheless wended its way into the heart of defense planning. The Air Force's cornerstones of information warfare, for example, has approached the status of doctrine. The spring 1996 establishment of the 609th Squadron (at Shaw Air Force Base) dedicated to information warfare offers further evidence of the seriousness with which that ideology is maintained. In 1996 the National Defense University (NDU) ended its two-year experiment of offering a forty-four-week program on Information Warfare and strategy after forty-eight students were graduated. In 1995-96 large portions of the defense budget were designated information operations (although only a small portion represents information warfare).

DESCRIPTORS: *INFORMATION SYSTEMS, *DEFENSE PLANNING, *NATIONAL DEFENSE, *INFORMATION WARFARE, AIR FORCE, DEPARTMENT OF DEFENSE, COMMUNITIES, AIR FORCE FACILITIES, MILITARY BUDGETS, MILITARY ORGANIZATIONS, DOCTRINE.

AD-A368079

RAND CORP SANTA MONICA CA

The People's Liberation Army in the Information Age

1999 295 PAGES

PERSONAL AUTHORS: Mulvenon, James C.; Yang, Richard H.

UNCLASSIFIED REPORT

ABSTRACT: (U) This volume is the product of a conference, jointly sponsored by the Rand Center for Asia-Pacific Policy (CAPP) and the Taiwan-Based Chinese Council of Advanced Policy Studies (CAPS), held in San Diego, California, from 9-12 July 1998. The meeting brought together Chinese military experts to discuss a subject too long ignored: The non-hardware side of the People's Liberation Army' s (PLA's) modernization. The result is a comprehensive examination of the critical "software" side of China's military modernization, covering topics as diverse as civil-military relations, professionalism, logistics, training, doctrine, systems integration, and force structure, where as financial and logistical support for the conference was supplied by CAPS and CAPP, funding for the publication of this volume was provided by Rand's Project Air Force Strategy and Doctrine program, under the leadership of Dr. Zalmay Khalilzad. This program is in the third year of a comprehensive study of issues related to Chinese military and security affairs for the United States Air Force; the project is entitled "Chinese Defense Modernization and its Implications for the U.S. Air Force." It focuses on the fundamental question of how U.S. policy should deal with China, a rising power that could have the capability, in the not too distant future, of challenging the U.S. position in East Asia and its military, political, and economic access to that dynamic and important region.

DESCRIPTORS: *UNITED STATES, *POLICIES, *MILITARY FORCES (FOREIGN), *MILITARY DOCTRINE, *MILITARY MODERNIZATION, *CHINA, LOGISTICS SUPPORT, MILITARY PERSONNEL, WARFARE, AIR FORCE, MILITARY STRATEGY, INTEGRATED SYSTEMS, TRAINING, SECURITY.

AD-A367983

AIR WAR COLL MAXWELL AFB AL

China as Peer Competitor? Trends in Nuclear Weapons, Space, and Information Warfare

JUL 1999 45 PAGES

PERSONAL AUTHORS: Gauthier, Kathryn L.

UNCLASSIFIED REPORT

ABSTRACT: (U) In China as peer competitor? Lt Col Kathryn L. Gauthier analyzes the potential for China to emerge as a peer competitor of the United States in the coming decades. First, she examines two traditional pillars of national strength--China's status as a nuclear weapons state and as a space power. Second, she explores China's growing focus on information warfare (IW) as a means to wage asymmetric warfare against a technologically advanced adversary. Third, the author carefully examines the status of the three programs, highlights areas of concern and potential conflict with the United States, and analyzes the implications of these issues for the United States.

DESCRIPTORS: *NUCLEAR WEAPONS, *CHINA, *INFORMATION WARFARE, NUCLEAR PROLIFERATION, WARFARE, UNITED STATES, POLICIES, FOREIGN TECHNOLOGY, SPACE SYSTEMS, CONFLICT, POWER, DOCTRINE.

AD-A367763

NATIONAL DEFENSE UNIV
WASHINGTON DC INST FOR
NATIONAL STRATEGIC STUDIES

The Mesh and the Net Speculations on Armed Conflict in a Time of Free Silicon

AUG 1995 172 PAGES

PERSONAL AUTHORS: Libicki, Martin C.

UNCLASSIFIED REPORT

ABSTRACT: (U) This report contains information concerning the impact of computer technology on future military conflicts.

DESCRIPTORS: *MILITARY MODERNIZATION, *UNCONVENTIONAL WARFARE, *INFORMATION WARFARE, MILITARY INTELLIGENCE, DISTRIBUTED DATA PROCESSING, COMBAT READINESS, THREAT EVALUATION, INTERNET, TECHNOLOGY FORECASTING.

AD-A367670

FYSISCH EN ELEKTRONISCH LAB TNO
THE HAGUE (NETHERLANDS)

Survey of Information Warfare, Information Operations and Information Assurance

JUL 1999 92 PAGES

PERSONAL AUTHORS: Luiijf, H. A. M.

UNCLASSIFIED REPORT

ABSTRACT: (U) Research survey on the phenomena information warfare, information operations (INFO OPS) and information assurance. History, development, definitions and developments in various countries around the globe. Appendix with list of abbreviations of terms in these fields.

DESCRIPTORS: *DATA PROCESSING SECURITY, *INFORMATION WARFARE, MILITARY OPERATIONS, NETHERLANDS, DUTCH LANGUAGE, SECURE COMMUNICATIONS, INFORMATION PROCESSING.

AD-A367662

NATIONAL DEFENSE UNIV
WASHINGTON DC INST FOR
NATIONAL STRATEGIC STUDIES

What is Information Warfare?

AUG 1995 110 PAGES

PERSONAL AUTHORS: Libicki, Martin C.

UNCLASSIFIED REPORT

ABSTRACT: (U) This essay examines that line of thinking and indicates several fundamental flaws while arguing the following points: Information warfare, as a separate technique of waging war, does not exist. There are, instead, several distinct forms of information warfare, each laying claim to the larger concept. Seven forms of information warfare-conflicts that involve the protection, manipulation, degradation, and denial of information-can be distinguished: (1) Command-and-control warfare (which strikes against the enemy's head and neck), (2) Intelligence-based warfare (which consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace), (3) Electronic warfare (radio-electronic or cryptographic techniques), (4) Psychological warfare (in which information is used to change the minds of friends, neutrals, and foes), (5) "Hacker" warfare (in which computer systems are attacked), (6) Economic information warfare (blocking information or channeling it to pursue economic dominance), and (7) Cyberwarfare (a grab bag of futuristic scenarios). All these forms are weakly related. The concept of information warfare has as much analytic coherence as the concept, for instance, of an information worker. The several forms range in maturity from the historic (that information technology influences but does not control) to the fantastic (which involves assumptions about societies and organizations that are not necessarily true).

DESCRIPTORS: *ELECTRONIC WARFARE, *DATA PROCESSING SECURITY, *INFORMATION WARFARE, WARFARE, NATIONAL SECURITY, RISK, INFORMATION SYSTEMS, THREATS, VULNERABILITY, COMMAND AND CONTROL SYSTEMS.

AD-A367661

NATIONAL DEFENSE UNIV
WASHINGTON DC INST FOR
NATIONAL STRATEGIC STUDIES

Defensive Information Warfare

AUG 1996 82 PAGES

PERSONAL AUTHORS: Alberts, David S.

UNCLASSIFIED REPORT

ABSTRACT: (U) The problem of defending against information warfare is real. Our citizens and the organizations that provide them with the vital services they need can find no sanctuary from these attacks. The low cost of mounting these attacks has enlarged the field of potential adversaries and complicated efforts to collect intelligence and array our defenses. The consequences of a well-planned and coordinated attack by a relatively sophisticated foe could be serious. Even the threat of such an attack or digital blackmail is a distinct possibility. How the public will respond to the threat of IW infrastructure attacks or to actual attacks is unclear, but is a major determinant of future policy and actions. This situation is getting worse with the rapid proliferation of information technology and know-how. We are becoming increasingly dependent on automation in every aspect of our lives. As information technology becomes an essential part of the way organizations and individuals create products and provide services, the need for interconnectivity and interoperability increases. With this increased need for exchanges of information (and products), vulnerabilities increase. Finally, the increased reliance on commercial-off-the-shelf products or commercial services makes it more and more difficult for organizations and individuals to control their own security environment.

DESCRIPTORS: *NATIONAL SECURITY, *DEFENSE PLANNING, *INFORMATION WARFARE, AUTOMATION, DEFENSE SYSTEMS, LOW COSTS, THREATS, OFF THE SHELF EQUIPMENT, COMMERCIAL EQUIPMENT, CATASTROPHIC CONDITIONS, ELECTRONIC SECURITY.

AD-A367312

AIR FORCE ACADEMY
COLORADO SPRINGS CO

Building Castles on Sand? Ignoring the Rip Tide of Information Operations

1 APR 1998 69 PAGES

PERSONAL AUTHORS: Bass, Carla D.

UNCLASSIFIED REPORT

ABSTRACT: (U) This paper will attempt to prove that a CINC for IO is now necessary to capture the plethora of ongoing IO related activities and hone them into a single, powerful, coordinated capability. Furthermore, using special operations command as a model, responsibility for IO should be assigned to an extent unified command. This additional mission should be accompanied by a designated program element to eliminate sporadic, uncoordinated, and oftentimes insufficient I0 expenditures, and to more efficiently distribute lessons learned across DoD.

DESCRIPTORS: *INFORMATION SYSTEMS, *MILITARY COMMANDERS, *INFORMATION WARFARE, MILITARY REQUIREMENTS, LESSONS LEARNED, COMBAT READINESS, THREAT EVALUATION, MILITARY MODERNIZATION.

AD-A367206

INSTITUTE FOR DEFENSE ANALYSES
ALEXANDRIA VA

Exercise Rainbow Serpent After Action Report

Jan 1999 31 Pages

PERSONAL AUTHORS: Lidy, A. Martin; Packer, Samuel H.

UNCLASSIFIED REPORT

ABSTRACT: (U) This document, the second in a series to be produced for the sponsor, provides an after action review of an Australian led multinational command post exercise focused on peace support operations. It identifies highlights of the exercise and provides a number of observations that respond to specific questions raised by the sponsor regarding: strengths and weakness of U.S. forces engaged in smaller-scale contingency operations; the other organizations with which U.S. forces will need to coordinate their activities when engaged in these operations; and the doctrine and structure implications of such operations.

DESCRIPTORS: *PEACETIME, *MILITARY EXERCISES, MILITARY DOCTRINE, STRUCTURES, INFORMATION WARFARE.

AD-M000657

JOINT STAFF WASHINGTON DC

Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance (Computer Diskette)

4 JUL 1996 14 PAGES

UNCLASSIFIED REPORT

ABSTRACT: (U) System requirements: PC compatible; Word 6.0; Windows. The performance of essential national security-related functional activities is increasingly dependent on U.S. infrastructures and their supporting information components. In view of the dependency, and because the Department of Defense (DoD) information infrastructure is embedded in larger national and international infrastructures, DoD officials, their advisors, and others within and outside the government have recommended to the national security council staff that this may be necessary to initiate interdepartmental/interagency discussions. Topics of such a dialogue would include the dependency and vulnerability issues and the need for national policy to deal with them. The report does, however, address the breadth and complexity of the policy and strategy issues and summarizes the views of those in positions of importance to the development of policy for infrastructure protection and assurance. The environmental areas examined were: (1) Infrastructures; (2) Legal Environment; (3) Regulatory Environment; (4) Policy Environment; (5) Technology Environment; and (6) Intelligence Environment.

DESCRIPTORS: *MAGNETIC DISKS, *DATA PROCESSING SECURITY, *ELECTRONIC WARFARE, *NATIONAL SECURITY.

AD-A368490

JOINT ADVANCED DISTRIBUTION SIMULATION/JOINT TEST AND EVALUATION ALBUQUERQUE NM

JADS Special Report on Networking & Engineering, Appendices A, B, C, D, & E

19 AUG 1999 205 PAGES

PERSONAL AUTHORS: Ashton, Charles P.

UNCLASSIFIED REPORT

ABSTRACT: (U) The Joint Advanced Distributed Simulation (JADS) Joint Test Force (JTF) was chartered by the Office of the Secretary of Defense to investigate the utility of Advanced Distributed Simulation (ADS) technology for Test and Evaluation (T&E). JADS executed three test programs; command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), precision guided munitions, and electronic warfare, representing slices of the overall T&E spectrum as well as observing other activity within the T&E community to form its conclusions. Each of the three tests required that T&E facilities be linked together through a communications network to support an ADS architecture. This report outlines the network design requirements, network description, and describes the components of the JADS communications network. Also, this report addresses JADS JTF costs, concerns and constraints, and lessons learned. It is intended to provide insight into the process JADS JTF undertook in setting up distributed communications networks capable of supporting ADS testing.

DESCRIPTORS: *COMPUTERIZED SIMULATION, *MILITARY INTELLIGENCE, *COMMAND CONTROL COMMUNICATIONS, *ELECTRONIC WARFARE, *SYSTEMS ENGINEERING, *COMMUNICATIONS NETWORKS, *SURVEILLANCE, *RECONNAISSANCE.

AD-A367655

NAVAL AIR WARFARE CENTER AIRCRAFT DIV PATUXENT RIVER MD

The ACETEF HLA Interface for JADS-EW

3 AUG 1999 8 PAGES

UNCLASSIFIED REPORT

ABSTRACT: (U) This paper presents the software approach taken at ACETEF to support the JADS-EW test. It begins by describing the overall structure of the JADS-EW federation and the roles played by the federates. The HLA interface consisted of two major components, namely the RTI interface and the SWET interface, designed to work together but separately, in order to decrease the workload of a single HLA interface. Though performing different functions, their general structure is similar in that each is guided by a federate manager, which directs all activity according to the specifications of a particular federation. Another common feature between both interfaces is the utilization of the C++ class inheritance, virtual functions, and polymorphism capabilities, which greatly assist in producing highly maintainable and reusable code.

DESCRIPTORS: *COMPUTER PROGRAMS, *ELECTRONIC WARFARE, *INTERFACES, *JET FIGHTERS, *RADIO JAMMING, SURVIVABILITY, CODING, SYSTEMS APPROACH, WORKLOAD, REUSABLE EQUIPMENT, POLYMORPHISM.

AD-A366257

ARMY COMMAND AND GENERAL STAFF COLL FORT LEAVENWORTH KS SCHOOL OF ADVANCED MILITARY STUDIES

Prowler Integration into USAF Strategic Attack and Air Interdiction Missions

17 DEC 1998 56 PAGES

PERSONAL AUTHORS: Hake, Michael F.

UNCLASSIFIED REPORT

ABSTRACT: (U) The importance of protecting limited aircraft assets cannot be overstated. The loss of a modern aircraft entails the probable loss of highly trained and experienced crews that took years to develop. Furthermore, if a target is missed because of defensive reactions to radar-guided weapons, the sortie is lost and the target will have to be attacked again, draining valuable resources from the war effort and risking the attack package all over again. Therefore, the jamming of early warning, ground-control intercept, and acquisition radars maximizes the success of strike packages by creating significant confusion and friction inside the command and control system of an adversary by denying critical intelligence on aircraft routes, altitudes, and timing. This friction slows an adversary's ability to respond to aerial attacks and therefore contributes directly to the preservation of experienced combat crews and aircraft. Joint publication 3-01.4 defines Electronic Warfare (EW) as “any military action involving the use of electromagnetic energy and directed energy to control the electromagnetic spectrum or to attack the enemy.” EW is further divided into three subcategories: Electronic Attack (EA), Electronic Protect (EP), and Electronic Warfare Support (ES). Moreover, the proliferation of radar-directed surface-to-air missile and anti-aircraft artillery threats continue to require the U.S. to maintain a robust EA capability.

DESCRIPTORS: *AIR DEFENSE, *ELECTRONIC WARFARE, *INTERDICTION, *MISSIONS, *AIR FORCE PLANNING, MILITARY OPERATIONS, ELECTRONICS, WARFARE.

AD-A366196

ARMY COMMAND AND GENERAL STAFF COLL FORT LEAVENWORTH KS SCHOOL OF ADVANCED MILITARY STUDIES

Pull, Push or Shove: Global Broadcast Service and Intelligence Support to Maritime Forces

17 DEC 1998 62 PAGES

PERSONAL AUTHORS: Carter, Stuart A.

UNCLASSIFIED REPORT

ABSTRACT: (U) The Department of Defense developed the Global Broadcast Service (GBS) to increase the amount of national and theater level information provided to deployed forces, resolving some shortcomings in information dissemination identified during the Gulf War. Using direct broadcast satellite technology, GBS is expected to deliver information at rates exponentially faster than what is available now. The broadcast service makes possible the near-simultaneous transfer of critical information to multiple users. While GBS may speed the flow of information, it does nothing to improve the quality of intelligence. Given the large capacity of GBS, intelligence managers may be under unreasonable pressures to release information to fill available bandwidth. The result could be more raw information for commanders, and less finished intelligence. GBS has constraints and limitations inherent in its design. Not all users in a theater will have access to high-capacity bandwidth at the same time. Where the GBS broadcast beams are positioned will determine who gets what level of GBS bandwidth. The small antenna size of GBS receive suites allow the lowest-level tactical forces to receive intelligence support previously only available at the flag-level. To make the best use of the technology, under the proposed dissemination architecture intelligence planners must take the time actively manage the flow of information they receive. GBS offers new and unique dissemination capabilities.

DESCRIPTORS: *MILITARY INTELLIGENCE, *DEPARTMENT OF DEFENSE, *GLOBAL, *INFORMATION TRANSFER, *RADIO BROADCASTING, *SATELLITE COMMUNICATIONS, *INFORMATION WARFARE.

AD-A366192

ARMY COMMAND AND GENERAL STAFF COLL FORT LEAVENWORTH KS SCHOOL OF ADVANCED MILITARY STUDIES

The Information Operations Coordination Cell-Necessary for Division Offensive Actions

16 DEC 1998 67 PAGES

PERSONAL AUTHORS: Carter, Rosemary M.

UNCLASSIFIED REPORT

ABSTRACT: (U) This monograph analyzes the need for a division Information Operations (IO) Coordination Cell during offensive military actions. The integrated concept team draft of FM 100-6, Information Operations: Tactics Techniques and Procedures, includes a division Information Operations Coordination Cell. The cell is responsible for integrating the components of information superiority (IS) to defeat the enemy's command, control, computers, communications, intelligence, surveillance and reconnaissance (C4ISR) while protecting friendly C4ISR. Their focus is the Information Operations segment that includes operational security (OPSEC), psychological operations (PSYOP), military deception, electronic warfare (EW), physical destruction, computer network attack (CNA), public affairs (PA), and civil affairs (CA). The monograph restricts the topic to offensive IO, or IO that attacks the enemy commander's ability to achieve his objectives. Also, the monograph limits the type of military action to offensive.

DESCRIPTORS: *MILITARY TACTICS, *PSYCHOLOGICAL OPERATIONS, *INFORMATION WARFARE.

AD-A365673

RAND CORP SANTA MONICA CA

Securing the U.S. Defense Information Infrastructure: A Proposed Approach

1999 179 PAGES

PERSONAL AUTHORS: Anderson, Robert H.; Feldman, Phillip M.; Gerwehr, Scott; Houghton, Brian; Mesic, Richard

UNCLASSIFIED REPORT

ABSTRACT: (U) This report addresses the survivability and assured availability of essential U.S. information infrastructures, especially when they are under various forms of "information warfare" attack. To the best of our knowledge, the term "minimum essential information infrastructure" (MEII) was coined by one of the authors (Mesic) as part of the planning for a series of "Day After in Cyberspace" information warfare exercises conducted from 1995 to the present under the direction of our RAND colleague Roger Molander. The idea is that some information infrastructures are so essential that they should be given special attention, perhaps in the form of special hardening, redundancy, rapid recovery, or other protection or recovery mechanisms. This report documents the findings of the first year of a study of the MEII concept, attempting to formulate some initial answers to these questions-or, if these are not the right questions, to ask and answer better ones. This report should be of interest to persons responsible for assuring the reliability and availability of essential information systems throughout the U.S. defense establishment, the U.S. critical infrastructure, and other organizations.

DESCRIPTORS: *MILITARY INTELLIGENCE, *NATIONAL SECURITY, *ELECTRONIC SECURITY, *INFORMATION WARFARE.

AD-A365127

GEORGE WASHINGTON UNIV
WASHINGTON DC SCHOOL OF LAW

The International Legal Limitations on Information Warfare

24 MAY 1998 85 PAGES

PERSONAL AUTHORS: O'Brien, Gregory J.

UNCLASSIFIED REPORT

ABSTRACT: (U) We live in an age that is driven by information. Technological breakthroughs are changing the face of war and how we prepare for war. Information war has no front line. Potential battlefields are anywhere networked systems allow access to oil and as pipelines, for example, electric power grids, telephone switching networks. In sum, the U.S. homeland may no longer provide a sanctuary from outside attack. A panel of Defense Department experts recently warned the nation about the prospect of an electronic Pearl Harbor, a crippling sneak attack on the nation's defense and civilian information systems in which "cyberterrorists" and other unknown assailants cripple the nation's, or the world's, computer-networked communications, financial, and national defense systems.

DESCRIPTORS: *LIMITATIONS, *INTERNATIONAL LAW, *INFORMATION WARFARE, ELECTRONICS, WARFARE, NATIONS, DEFENSE SYSTEMS, INFORMATION SYSTEMS, NETWORKS.

AD-A364870

ODYSSEY RESEARCH ASSOCIATES INC
ITHACA NY

Task-Based Authorizations

APR 1999 74 PAGES

PERSONAL AUTHORS: Thomas, Roshan K.; Sandhu, Ravi; Das, Souvik

UNCLASSIFIED REPORT

ABSTRACT: (U) In this project we developed a new paradigm for access control and security models called task-based authorization controls (TBAC). This new authorization control paradigm is particularly suited for emerging models of computing, especially distributed computing and information processing activities with multiple points of access control and decision making. TBAC articulates security issues at the application and enterprise level. As such, it takes a task-oriented or transaction-oriented perspective rather than a perspective based upon traditional subject-object distinctions. In TBAC, access mediation involves authorizations at various points during the completion of tasks in accordance with the application logic associated with the overall governing process. In contrast, the subject-object view typically divorces access mediation from the larger context in which a subject performs an operation on an object. By taking a task-oriented view of access control and authorizations, TBAC lays the foundation for research into a new breed of "active" security models. TBAC has broad applicability to access control, ranging from fine-grained activities such as client-server interactions in a distributed system, to coarser units of distributed applications and workflows that cross departmental and organizational boundaries.

DESCRIPTORS: *DISTRIBUTED DATA PROCESSING, *DATA PROCESSING SECURITY, *INFORMATION WARFARE.

AD-A364072

ARMY WAR COLL
CARLISLE BARRACKS PA

The Impact of Computer Network Attacks on Infrastructure Centers of Gravity

7 APR 1999 29 PAGES

PERSONAL AUTHORS: Payne, Allan D.

UNCLASSIFIED REPORT

ABSTRACT: (U) Computer network attack is a significant asymmetric threat to the United States and its military. Motives vary, but the threat from CNA is real; U.S. infrastructure targets are vulnerable; those that directly affect the ability of the U.S. military to conduct its missions are evident innovation in CNA is unrestrained, and privacy rights of the U.S. citizenry conflict directly with U.S. Government efforts to take active measures to help defend against CNA. CNA today could be economically damaging to the computer and network dependent society that the United States has become. The challenge is to define the problem separately from every other consideration and challenge that the military faces in the information age including the broader mission areas of information operations and information warfare.

DESCRIPTORS: *COMPUTER NETWORKS, *INFRASTRUCTURE, *INFORMATION WARFARE, UNITED STATES, STRATEGY, DAMAGE, THREATS, COMPUTERS, ATTACK, TARGETS, MISSIONS.

AD-A364003

RAND CORP SANTA MONICA CA

The Changing Role of Information in Warfare

1998 462 PAGES

PERSONAL AUTHORS: Khalilzad, Zalmay M.; White, John P.

UNCLASSIFIED REPORT

ABSTRACT: (U) This effort to assess how the role of information in warfare is changing seeks to understand many of the remarkable developments under way in information and communications technology, and their potential effects on warfare. Indeed, this volume reveals several important lessons that can be gleaned from the very different and distinct perspectives contained in it: Information advances will affect more than just how we fight wars. The nature and purpose of war itself may change. How wars start, how they end, their length, and the nature of the participants may change as shifts in the relative power of states and nonstate entities occur. New technologies cut both ways in terms of their effects on national security. Together, the chapters make clear that advances create new vulnerabilities; new threats create new opportunities.

DESCRIPTORS: *COMPUTER PROGRAMS, *DEFENSE SYSTEMS, *INFORMATION WARFARE, WARFARE.

AD-A363260

NAVAL WAR COLL NEWPORT RI JOINT MILITARY OPERATIONS DEPT

Command and Control in Joint Vision 2010: Flexible, Adaptive and Networked

5 FEB 1999 25 PAGES

PERSONAL AUTHORS: Olmo, Frank J.

UNCLASSIFIED REPORT

ABSTRACT: (U) One of the most daunting tasks the U.S. Military will face in the 21st century is the issue of implementing effective command and control (C2) of joint and coalition military operations. As new technologies are implemented to support Joint Vision 2010 (JV2010), successful C2 must give the commander the flexibility to use faster and more accurate information technologies in order to increase battlespace knowledge and situational awareness. The dynamics of new technologies is linked to the information age and is commonly referred to as a Revolution in Military Affairs (RMA), which is leveraged through the enabling concepts of "Information Superiority" and "Network-Centric Warfare." The challenge for the future commander is to exploit the RMA by applying a flexible C2 process to control the battlespace. Thus, as networked forces bring faster and more accurate information across all levels of war, the operational commander will exert his influence by maintaining a flexible networked architecture through a continuum based on his intent and the tempo of operations. A more focused understanding of networked C2 is the key to the evolution of new and existing joint architectures in order to keep pace with information technologies.

DESCRIPTORS: *COMMAND AND CONTROL SYSTEMS, *JOINT MILITARY ACTIVITIES, INFORMATION EXCHANGE.

AD-A360466

DYNETICS INC SHALIMAR FL

Linking Advanced Distributed Simulations with Flight Testing

JUL 1997 11 PAGES

PERSONAL AUTHORS: Ayers, Douglas S.; Cross, Robert; Fox, Brian; Hostilo, Wayan; Pappas, Johnny

UNCLASSIFIED REPORT

ABSTRACT: (U) The Test and Evaluation community is relatively new to Advanced Distributed Simulation technology (ADS). Each facility participating in the JADS program has independently developed a method for testing specific aspects of various weapons systems. The MISILAB, which organizationally is part of the OWEF, but is located in a separate facility, has supported AMRAAM simulations and characterizations over the past decade. The CCF has supported real-time mission control, and monitoring functions providing pre- and post-flight analysis in the DoD community for the past 40 years. The Primes Test Facility has been involved in the ground testing of munitions systems, Electronic Warfare (EW), and Electromagnetic Interference (EMI)/Electromagnetic Compatibility Testing (EMC) for the past 17 years. The challenge was to develop a network architecture which would interface to the legacy systems in each test facility in a real-time distributed environment.

DESCRIPTORS: *FLIGHT TESTING, *DISTRIBUTED INTERACTIVE SIMULATION, ELECTRONIC WARFARE, MONITORING, NETWORKS, REAL TIME, WEAPON SYSTEMS, TEST METHODS, MISSIONS, ELECTROMAGNETIC INTERFERENCE, AMMUNITION, FLIGHT SIMULATORS, ELECTROMAGNETIC COMPATIBILITY.

AD-A359912

NAVAL POSTGRADUATE SCHOOL
MONTEREY CA

Unattended Ground Sensors and Precision Engagement

DEC 1998 215 PAGES

PERSONAL AUTHORS: Haider, Eric D.

UNCLASSIFIED REPORT

ABSTRACT: (U) Unattended Ground Sensors (UGS) are devices that automatically gather sensor data on a remote target, interpret the data and communicate information back to a receiver without interaction with a human operator. The objective of this thesis is to determine how unattended ground sensor technologies might support precision engagement. Comparative case analysis of the use of sensors in Vietnam, the Sinai and Iraq is used to develop principles that UGS must meet to support precision engagement. This study finds that precision engagement requires long endurance UGS to be delivered covertly to discriminate between targets, interrogate them for emissions, while disseminating a fused picture of the target. This study details roles and missions which UGS can fill as well as their costs, benefits and unintended consequences.

DESCRIPTORS: *DETECTORS, *HORIZON SCANNERS, *INFORMATION WARFARE, MILITARY INTELLIGENCE, GROUND LEVEL, EMISSION, THESES, TARGETS, COSTS, ENDURANCE (GENERAL), PRECISION, OPERATORS (PERSONNEL), REMOTE AREAS.

AD-A359702

NAVAL POSTGRADUATE SCHOOL
MONTEREY CA

Vision Guidance Controller for an Unmanned Aerial Vehicle

DEC 1998 94 PAGES

PERSONAL AUTHORS: Watson, Mark T.

UNCLASSIFIED REPORT

ABSTRACT: (U) The use of Unmanned Aerial Vehicles (UAVs) in modern military operations for reconnaissance and other missions continues to grow. UAV systems using remote control guidance are limited in range and subject to electronic warfare concerns. Guidance systems using only Global Positioning Service (GPS) or an Inertial Navigation System (INS) are limited to a pre-programmed route of flight. A vision guidance system that can control the UAV over an arbitrary course is not subject to these limitations. This thesis uses classical control methods to develop and test an autonomous vision controller for the Fog-R UAV (FROG). First, a computer model of the camera output for a flight that tracks a river is made to develop the controller and to test it in nonlinear simulation. Finally, the complete system is flight tested on the Fog R UAV. The design and test equipment include a highly modified Fog-R UAV from the U.S. Army, the Matrixx Product Family of software tools developed by Integrated Systems, Inc., and a ground station built at NPS from commercially available computer and communication equipment.

DESCRIPTORS: *MILITARY OPERATIONS, *UNMANNED, *GUIDANCE, COMPUTER PROGRAMS, COMPUTERIZED SIMULATION, SIMULATION, ELECTRONIC WARFARE, INTEGRATED SYSTEMS.

AD-A358442

JOINT ADVANCED DISTRIBUTION SIMULATION/JOINT TEST AND EVALUATION ALBUQUERQUE NM

High Level Architecture Runtime Infrastructure Test Report

AUG 1998 52 PAGES

PERSONAL AUTHORS: Wright, D. L.; Harris, Clyde J.; Black, Jerry W.

UNCLASSIFIED REPORT

ABSTRACT: (U) Joint Advanced Distributed Simulation Joint Test and Evaluation is an Office of the Secretary of Defense sponsored joint test force chartered to determine the utility of advanced distributed simulation (ADS) technologies for Test and Evaluation (T&E). The JADS EW test will use High Level Architecture (HLA) federates to replicate all elements of an actual open air range (OAR) test environment and the selected EW system under test. To determine the utility of ADS technology for EW T&E, JADS will use and evaluate the HLA in a three phase test program. During the ADS test phases, each OAR test run will be recreated using HLA compliant federates. This report addresses performance of a key HLA component developed by the Defense Modeling and Simulation Organization (DMSO) called the Runtime Infrastructure (RTI). Use of the RTI is required to be HLA compliant. Since the RTI provides a new means for dissimilar simulators and facilities to communicate, an additional source of latency is imposed on a test architecture which must be measured, optimized, and controlled for accurate real time measurement of test events. This work was performed for the JADS EW test and is the subject of this report.

DESCRIPTORS: *ELECTRONIC WARFARE, *DISTRIBUTED INTERACTIVE SIMULATION, *COMBAT SIMULATION, ALGORITHMS, COMPUTER COMMUNICATIONS, REAL TIME, COMPUTER ARCHITECTURE, COMPUTER NETWORKS.

AD-A357635

JOINT CHIEFS OF STAFF
WASHINGTON DC

Joint Doctrine for Command and Control Warfare (C2W)

7 FEB 1996 100 PAGES

UNCLASSIFIED REPORT

ABSTRACT: (U) This publication concentrates on command and control warfare (C2W) and is not intended to present comprehensive doctrine for the broader concept of Information Warfare (IW). It introduces and defines IW in general terms with the objective of clarifying its overarching relationship to C2W. The scope of C2W is defined in the Chairman of the Joint Chiefs of Staff Memorandum of Policy 30, but the full dimensions of IW policy and its implementation are still emerging.

DESCRIPTORS: *COMMAND AND CONTROL SYSTEMS, *INFORMATION WARFARE, MILITARY INTELLIGENCE, MILITARY DOCTRINE, JOINT MILITARY ACTIVITIES.

AD-A357499

JOINT CHIEFS OF STAFF
WASHINGTON DC

Joint Intelligence Support to Military Operations

20 NOV 1996 174 PAGES

UNCLASSIFIED REPORT

ABSTRACT: (U) This publication establishes doctrinal guidance on the provision of intelligence products, services, and support to joint operations. It provides the fundamentals of joint intelligence operations, addressing organization of joint intelligence forces, responsibilities, and command relationships. The focus will be joint intelligence support to combatant commanders revolving around the phases of the intelligence cycle: planning and direction, collection, processing and exploitation, production; dissemination and integration and evaluation. Finally, personnel, physical, operations and communications security considerations will be addressed. Joint intelligence doctrine defines the roles and relationships of intelligence organizations at the national level, in the combatant commands, and in the subordinate joint forces. The goal is to maximize the impact of intelligence while increasing effectiveness among the organizations that support the Joint Force Commander (JFC). Intelligence plays a critical role across the range of military operations from peace to war. Intelligence enables commanders at all levels to focus their combat power and resources and to provide force protection for those resources.

DESCRIPTORS: *MILITARY INTELLIGENCE, *COMBAT EFFECTIVENESS, *JOINT MILITARY ACTIVITIES, *MILITARY PLANNING, MILITARY DOCTRINE, INFORMATION WARFARE.

AD-A355904

NAVAL POSTGRADUATE SCHOOL
MONTEREY CA

Operationalization of Information Technology for the 21st Century (IT-21): The Flight Scheduling Function in Patrol Squadron 40 as a Case Study

SEP 1998 81 PAGES

PERSONAL AUTHORS: Flatau, Richard P., Jr

UNCLASSIFIED REPORT

ABSTRACT: (U) In the past several years, greater exploitation of information technology to increase leverage of information has become a central focus in the military. This focus is reflected in a number of strategic vision documents. Two significant examples are "Joint Vision 2010" signed in 1996 by the Chairman of the Joint Chiefs of Staff and the 1997 Quadrennial Defense Review Report. Achieving and using information superiority is seen as essential to future military success. This has led to the emergence of a new warfare paradigm: network-centric warfare. Towards this end, the Navy's service-wide IT improvement initiative is information technology for the 21st century (IT-21). IT-21 establishes a standard for it capability to be achieved throughout the Navy within which Navy units can shape their IT improvements. This study explores a requirements-approach for planning improvement of it through IT-21. Specifically, it focuses on a single function of one squadron: Flight scheduling in Patrol Squadron 40. This study addresses how to establish information requirements, assess current IT performance, and formulate specifications by which to drive planning for IT improvement. It concludes by mapping IT-21 components to requirements to provide VP-40 with a plan for improving its flight scheduling process through IT-21.

DESCRIPTORS: *INFORMATION SYSTEMS, *SCHEDULING, AIR TRAFFIC CONTROL SYSTEMS, SYSTEMS ANALYSIS, INFORMATION WARFARE.

AD-A355203

ELECTRO-RADIATION INC TOTOWA NJ

EW Testing Lessons Learned

16 JUN 1998 14 PAGES

PERSONAL AUTHORS: Berkowitz, Paul H.

UNCLASSIFIED REPORT

ABSTRACT: (U) Electronic Warfare (EW) testing is one of the more challenging undertakings in the Avionics community. EW tests are typically fraught with a myriad of problems due to the inherent complexity of tests involving multiple vehicles, radars, data collection, and data processing, as well as the complex nature of electronic warfare itself. Electro-Radiation Inc. (ERI) has been at the forefront of EW testing for many years, from B-52 to B-2 and from F-101 to F-22. While it is impossible to prevent all problems, it is possible to prevent the same problems from repeating. This paper applies many of the lessons ERI learned from its extensive EW testing experience, and offers recommendations of how to avoid repeating them. Electro-Radiation Inc. (ERI) has been a leader in the field of Electronic Warfare (EW) testing for many years.

DESCRIPTORS: *AVIONICS, *FLIGHT TESTING, *ELECTRONIC WARFARE, *AIRCRAFT EQUIPMENT, TEST AND EVALUATION, DATA PROCESSING.

AD-A355202

AIR FORCE RESEARCH LAB
WRIGHT-PATTERSON AFB OH

Changing Requirements for EW Threat Simulation

22 OCT 1998 10 PAGES

PERSONAL AUTHORS: Eberl, Edward G.

UNCLASSIFIED REPORT

ABSTRACT: (U) This paper represents my own observations based on recent procurement and contract activity engaged in by Amherst Systems. It is not the result of a scientific survey. No requirement is intended to be associated with a specific system under test or program. These observations are based on many recent requests for proposals and contracts which Amherst Systems has been exposed to. As a leading manufacturer of EW threat simulators for all applications (RWRs, Jammers, Elint Receivers, etc.), Amherst Systems is in a unique position to be aware of many current and future requirements.

DESCRIPTORS: *COMPUTERIZED SIMULATION, *ELECTRONIC WARFARE, *THREATS, *THREAT EVALUATION, SCANNING, SIMULATORS, WAVEFORMS, ELECTROMAGNETIC RADIATION, SIGNALS, RADIOFREQUENCY, APERTURES, TRANSMITTER RECEIVERS, ELECTRONIC INTELLIGENCE.

AD-A354665

ARMY RESEARCH LAB
ABERDEEN PROVING GROUND MD

Vulnerability Assessment of the InterNetwork Controller (INC)

SEP 1998 33 PAGES

PERSONAL AUTHORS: Retter, Charles; Gwyn, Douglas

UNCLASSIFIED REPORT

ABSTRACT: (U) The Tactical Internet (TI) provides a reliable digital communications infrastructure for Task Force XXI at brigade level and below. The InterNetwork controller (INC) performs routing and protocol conversion of data traffic within the TI, so its vulnerabilities could have significant adverse effects on the flow and content of data communications within the TI. This report summarizes the results of a study of potential "information warfare" vulnerabilities of the INC's interfaces, configuration, protocols, procedures, and policies.

DESCRIPTORS: *VULNERABILITY, *COMPUTER NETWORKS, *DIGITAL COMMUNICATIONS, *INFRASTRUCTURE, *INFORMATION WARFARE, CONVERSION, DIGITAL SYSTEMS, POLICIES, DATA TRANSMISSION SYSTEMS, TRAFFIC, BRIGADE LEVEL ORGANIZATIONS, TASK FORCES, DAMAGE ASSESSMENT, ADVERSE CONDITIONS, RELIABILITY (ELECTRONICS).

AD-A354205

AIR FORCE INST OF TECH
WRIGHT-PATTERSON AFB OH

Feasibility Study on the Use of the Internet for Traffic of Unclassified Data

SEP 1998 160 PAGES

PERSONAL AUTHORS: Guerra, Alexandre L.; Gustavo, Luis; Silva, F. P.

UNCLASSIFIED REPORT

ABSTRACT: (U) This research compares two possible networking methods for connecting all Brazilian Air Force Materiel Command units responsible for support and operation of Brazilian Air Force's weapons systems. The network includes the use of dedicated X.25 links, and the use of a virtual private network using the internet (TCP/IP) as the medium of transmission. The Brazilian Air Force Materiel Command, responsible to support operating units over a very large sparse territory, lacks an efficient media of computer communications, which makes it difficult to control the supply chain channels of materiel present in each unit, depots, and warehouses. We studied the network infrastructure necessary to solve this problem, and proposed two different scenarios. One uses the current level of technology based on dedicated X.25 environment, and the other uses the incipient virtual private networking technology and the internet as the communication medium. The results suggest that the Brazilian Air Force could be able to use the internet and VPN technology in a moderated secure environment (C2 Level), and could save more than $100,000 per month in comparison to the implementation of the same level of networking using the present X.25 model.

DESCRIPTORS: *COMPUTER COMMUNICATIONS, *LOGISTICS MANAGEMENT, *INTERNET, COST EFFECTIVENESS, DISTRIBUTED DATA PROCESSING, SECURITY, COMMUNICATIONS TRAFFIC, INFORMATION WARFARE.

AD-A351744

NAVAL POSTGRADUATE SCHOOL
MONTEREY CA

Construction and Measurement of an Actively Mode-Locked Sigma Laser

JUN 1998 165 PAGES

PERSONAL AUTHORS: Butler, James M.

UNCLASSIFIED REPORT

ABSTRACT: (U) The direct digitization of microwave signals of interest would allow rapid computer processing and analysis. Current analog-to-digital converters (ADCs) are bandwidth limited and electronic warfare systems must down-convert the signal before digitization causing a loss of information. optical ADCs can directly digitize frequencies greater than 10 GHz using wideband integrated optical interferometers (folding ADCs). A critical component of the optical folding ADC is the pulsed laser used for sampling the wideband signal. The amplitude-modulated pulses become the discrete samples of the analog signal. Limiting factors in an optical ADC are the pulse width, the pulse rate, and the jitter noise of the optical pulse train. Mode-locked lasers provide pulse rates and pulse widths suitable for high bandwidth applications. In this thesis a mode-locked sigma laser was constructed using fiber-optic, electro-optic, and microwave components. The theory of mode-locking, laser construction, output measurements, and sampling applications are discussed in detail.

DESCRIPTORS: *MEASUREMENT, *CONSTRUCTION, *MODE LOCKED LASERS, DIODES, FIBER OPTICS, OPTICAL PROPERTIES, SYSTEMS, COMPUTERS, MICROWAVE EQUIPMENT, PULSED LASERS, LASERS, PHASE, PULSE RATE, OPTICAL INTERFEROMETERS, BROADBAND, AMPLITUDE MODULATION, PULSE TRAINS.

AD-A351710

NAVAL WAR COLL NEWPORT RI

Weapons of Mass Destruction a Network-Centered Threat

18 MAY 1998 23 PAGES

PERSONAL AUTHORS: Diggs, D. G.

UNCLASSIFIED REPORT

ABSTRACT: (U) Battlespace dominance is more than the physical control of air, land, and sea. Under the network centric concept of operations, U.S. forces must be ready to control the infosphere in order to assure military objectives can be achieved. Perhaps the most effective information warfare (IW) weapon is a weapon of mass destruction (WMD), specifically a biological or nuclear weapon. Important questions should be answered about the ability to protect American information networks from the significant information disruption characteristics of WMD.

DESCRIPTORS: *COMMAND CONTROL COMMUNICATIONS, *MASS DESTRUCTION WEAPONS, *INFORMATION WARFARE, MILITARY STRATEGY, MILITARY DOCTRINE, THREAT EVALUATION, COMPUTER NETWORKS, NATIONAL DEFENSE, DETERRENCE.

AD-A351431

MILITARY OPERATIONS RESEARCH SOCIETY ALEXANDRIA VA

66TH MORSS: Preparing for Military Operations Research in the 21st Century. Final Program and Book of Abstracts

20 MAY 1998 329 PAGES

PERSONAL AUTHORS: Kee-Lafreniere, Cynthia

UNCLASSIFIED REPORT

ABSTRACT: (U) This publication contains titles of presentations made at the 66th MORSS Symposium (66th MORSS), along with names, addresses, phone and fax numbers and e-mail addresses of authors, if available. In addition, abstracts of presentations, which are unclassified and approved for public release, are included. Some abstracts are missing because they had not been cleared for public release at the time of publication.

DESCRIPTORS: *MILITARY OPERATIONS, COMPUTERIZED SIMULATION, AIR DEFENSE, ELECTRONIC WARFARE, MILITARY PERSONNEL, LAND WARFARE, SYMPOSIA, INFORMATION SYSTEMS, COST ANALYSIS, OPERATIONAL READINESS, MANPOWER UTILIZATION, ABSTRACTS, LOGISTICS, WAR GAMES, INFORMATION WARFARE.

AD-A351075

ARMY WAR COLL
CARLISLE BARRACKS PA

In Support of Information Dominance: Acquisitions and Organizations

15 APR 1998 46 PAGES

PERSONAL AUTHORS: Kaura, Mary A.

UNCLASSIFIED REPORT

ABSTRACT: (U) The purpose of this work is to provide a basis and a framework for today's command, control, computer, communications, and intelligence (C4I) acquisition policies that will ensure the military is positioned to support success on the 21st century battlefield. This paper establishes an approximation of future warfare and the changing nature of organizational structures by summarizing current published works. Resulting tenets for C4I operations are then developed. A summary of the technical constraints that are related to and important for the implementation of the C4I tenets are provided. Specifically considered are technology hurdles in bandwidth, computer technology, and software complexity. Finally, current and recommended acquisition policies that are applicable to the success of C4I architectures in support of 21st century warfare are discussed.

DESCRIPTORS: *INFORMATION SYSTEMS, *MILITARY PROCUREMENT, *MILITARY ORGANIZATIONS, *INFORMATION WARFARE, SOFTWARE ENGINEERING, COMMAND CONTROL COMMUNICATIONS, MILITARY REQUIREMENTS, POLICIES, INFORMATION TRANSFER, COMPUTERS, TECHNOLOGY FORECASTING, COMBAT INFORMATION CENTERS, ELECTRONIC INTELLIGENCE.

AD-A350908

FLORIDA STATE UNIV TALLAHASSEE

The Effects of Truth Bias on Artifact-User Relationships: An Investigation of Factors for Improving Deception Detection in Artifact Produced Information

7 AUG 1998 201 PAGES

PERSONAL AUTHORS: Biros, David P.

UNCLASSIFIED REPORT

ABSTRACT: (U) A number of studies have been accomplished examining the truth bias individuals have toward others with whom they have a close relationship or familiarity (Mccornack and Parks, 1986; Levine and Mccornack, 1992; Stiff Kim and Ramesh, 1992). However, little has been done to examine the relationship between individuals and information artifacts. Does truth bias affect an individual's ability to detection strategic information manipulation in artifact-produced information? Are there measures that can be taken to improve the deception detection capabilities of artifact users? This research examines the artifact-user relationship and proposes a research model depicting the competing nature of artifact truth bias and detection factors such as experience, arousal and training as they influence an individual's ability to detect deception in artifact-produced information. The model was empirically tested in a laboratory experiment that included the use of a survey instrument. Together, the information collecting methods are used to gain a better understanding of the factors involved in strategic information manipulation and deception detection via artifacts.

DESCRIPTORS: *DATA PROCESSING SECURITY, *DECEPTION, *INFORMATION WARFARE, DATA MANAGEMENT, INFORMATION TRANSFER, COMPUTER COMMUNICATIONS, VULNERABILITY, THESES, HEURISTIC METHODS, MAN COMPUTER INTERFACE, ERROR DETECTION CODES.

◆**AD**-A350433

INFORMATION ASSURANCE TECHNOLOGY ANALYSIS CENTER MCLEAN VA

Information Assurance Technology Analysis Center. Information Assurance Tools Report. Vulnerability Analysis

1998 46 PAGES

UNCLASSIFIED REPORT

ABSTRACT: (U) This report provides an index of vulnerability analysis tool descriptions contained in the IATAC information assurance tools database. This report summarizes pertinent information, providing users with a brief description of available tools and contact information. It does not endorse or evaluate the effectiveness of each tool. As a living document, this report will be updated periodically as additional information is entered into the information assurance tools database.

DESCRIPTORS: *DATA PROCESSING SECURITY, *VULNERABILITY, DATA BASES, SOFTWARE ENGINEERING, DATA MANAGEMENT, COMPUTER COMMUNICATIONS, INFORMATION WARFARE.

AD-A348564

NAVAL WAR COLL NEWPORT RI JOINT MILITARY OPERATIONS DEPT

Joint Vision 2010: Information Superiority and its Effect on the Command and Control Process

13 FEB 1998 20 PAGES

PERSONAL AUTHORS: Ellis, Jeffrey A.

UNCLASSIFIED REPORT

ABSTRACT: (U) With the implementation of Joint Vision 2010, information superiority will impact every aspect of operational art, but none will be so great as the impact on operational command and control. Through information superiority, the operational commander theoretically gains a clearer picture of the battlespace, thus mitigating the fog of war. This study examines some of the potential command and control issues facing the operational commander as he attempts to conduct major operations and campaigns. Given the diverse threat, it is doubtful that U.S. forces can gain and maintain information superiority over our enemies. The need for information superiority will hamper our ability to operate in a combined environment. Information superiority may lead to operational command and control that is too rigid and too centralized to maintain friendly freedom of action. Operational commanders may become transfixed by increasing levels of information focusing on data instead of the application of forces in space and time. In the end, information superiority will provide a clearer picture of the battlespace but it will not mitigate the fog of war.

DESCRIPTORS: *MILITARY INTELLIGENCE, *DECISION MAKING, *COMMAND AND CONTROL SYSTEMS, *BATTLE MANAGEMENT, *INFORMATION WARFARE, THREATS, MILITARY COMMANDERS.

◆Included in the DTIC Review, March 2000

AD-A348473

NAVAL WAR COLL NEWPORT RI

The Double Edged Sword: Information Superiority or Information Vulnerability of Joint Vision 2010

13 FEB 1997 30 PAGES

PERSONAL AUTHORS: Tenner, Nancy L.

UNCLASSIFIED REPORT

ABSTRACT: (U) Joint Vision 2010 emphasizes the criticality of achieving information superiority in future military operations. With the global explosion of information age technology, the United States seeks a strategic and operational advantage through information while simultaneously denying an enemy any advantage. With no peer competitor to challenge the United States, adversarial nations may attempt to leverage the low cost, compared to high advantage, that information warfare has to offer. As the United States becomes increasingly reliant on the rapid flow of information, will the underlying infrastructure and deterrence effort provide sufficient security to ward off potentially devastating information warfare attacks? Operational Risk Management (ORM) is a methodology to identify hazard severity and probability from which to draw reasonable measures to reduce risk. (ORM) techniques can be adopted to assess information warfare (defense) hazards and assist in developing controls to minimize risks. Recommendations highlight the importance of educating personnel in information warfare, incorporating information warfare (defense) in war games, studying information infrastructure issues and applying ORM principles to reduce vulnerabilities.

DESCRIPTORS: *THREAT EVALUATION, *INFORMATION WARFARE, *RISK ANALYSIS, MILITARY INTELLIGENCE, NATIONAL SECURITY, MILITARY CAPABILITIES.

◆**AD-**A345705

ARMY WAR COLL
CARLISLE BARRACKS PA

Cyber-Terrorism: Modem Mayhem

14 APR 1998 40 PAGES

PERSONAL AUTHORS: White, Kenneth C.

UNCLASSIFIED REPORT

ABSTRACT: (U) America can no longer rely on broad oceans and a strong military to protect its homefront. The arrival of the information age has created a new menace cyber terrorism. This threat recognizes no boundaries, requires minimal resources to mount an attack, and leaves no human footprint at ground zero. This study addresses technology, identification procedures, and legal ambiguity as major issues, for countering cyber terrorism as an emerging challenge to U.S. national security. As America's reliance on computer technology increases, so does its vulnerability to cyber attacks.

DESCRIPTORS: *NATIONAL SECURITY, *ELECTRONIC SECURITY, *TERRORISM, DATA MANAGEMENT, COMPUTER COMMUNICATIONS, VULNERABILITY, THREAT EVALUATION, COUNTERTERRORISM, INFORMATION WARFARE.

◆ Included in the DTIC Review, March 2000

◆**AD**-A345602

ARMY WAR COLL
CARLISLE BARRACKS PA

The Department of Defense and the Age of Information Operations

13 MAY 1998 33 PAGES

PERSONAL AUTHORS: Evans, Alan T.

UNCLASSIFIED REPORT

ABSTRACT: (U) This paper explains the challenges and vulnerabilities the nation and especially the military will face in the next century as our dependence on information systems and associated infrastructure continues to grow. It will highlight the results of the President's commission on Critical Infrastructure Protection and discuss the steps necessary to protect the information systems upon which we have come to so heavily depend. It will highlight that without a comprehensive national policy in protecting information infrastructures poses a great risk to its military, commercial users and ultimately the nation.

DESCRIPTORS: *MILITARY OPERATIONS, *INFORMATION SYSTEMS, *MILITARY RESEARCH, DEPARTMENT OF DEFENSE, UNITED STATES GOVERNMENT, DATA MANAGEMENT, VULNERABILITY, PROTECTION, TECHNOLOGY FORECASTING, INFRASTRUCTURE, INFORMATION WARFARE.

AD-A345540

ARMY WAR COLL
CARLISLE BARRACKS PA

Managing Risk to the National Information Infrastructure

8 APR 1998 39 PAGES

PERSONAL AUTHORS: Thomas, James H.

UNCLASSIFIED REPORT

ABSTRACT: (U) Now, more than ever, the survival of our information based society depends on the integrity of our National Information Infrastructure (NII). Our information systems are vulnerable to a wide spectrum of threat ranging from a dissatisfied employee to a coordinated transnational attack to gain strategic advantage. Interconnected military, government and civilian information systems throughout our critical infrastructures, with limited self-protection features, are susceptible and attractive targets. The NII suffers attack almost constantly and we must do better at dealing with the consequences of such attacks. The ends, ways and means of managing the consequences of malevolent intrusion into the NII are within the capabilities of the nation to implement. Our success at dealing with these assaults, thus preventing an adversary from gaining strategic advantage jeopardizing our way of life will hinge on taking action to resolve the technological, legal, and sociological impediments to information infrastructure protection.

DESCRIPTORS: *NATIONAL SECURITY, *MANAGEMENT INFORMATION SYSTEMS, *DATA PROCESSING SECURITY, COMPUTER PROGRAMS, MILITARY INTELLIGENCE, ELECTRONIC WARFARE, INFORMATION EXCHANGE, COMPUTER COMMUNICATIONS, VULNERABILITY, PROTECTION, INTRUSION, INFRASTRUCTURE.

◆Included in the DTIC Review, March 2000

AD-A342718

ARMY WAR COLL
CARLISLE BARRACKS PA

Information Warfare Force XXI Situational Awareness

6 MAR 1998 44 PAGES

PERSONAL AUTHORS: Thomas, Laurence E., Jr

UNCLASSIFIED REPORT

ABSTRACT: (U) The 80's saw the introduction of stovepipe digital architectures in the primary combat arms branches (Aviation, Armor, Artillery, and Infantry) weapon systems. Some of these systems were not interoperable due to their unique software protocols. Aviation and artillery platforms were interoperable since they utilized the same protocol. In the 90's, General Sullivan expounded on his force XXI vision to digitally link all the combat arms horizontally and vertically to increase situational awareness. The materiel and combat developments communities produced an internet type system for the combat arms to provide situational awareness. An applique system was installed on some of the platforms so the weapons systems could digitally communicate within the internet. The applique system proposed to solve the stovepipe architectures will not work. Each combat arms system (AH-64D, MLA2 Abrams, M3 Bradley, Paladin/Crusader) has limited space, weight, and power constraints which prevent the integration of the applique system.

DESCRIPTORS: *WEAPON SYSTEMS, *INFORMATION WARFARE, COMPUTER PROGRAMS, MILITARY OPERATIONS, LESSONS LEARNED, INFORMATION SYSTEMS, DIGITAL COMMUNICATIONS, AWARENESS.

AD-A342284

ARMY WAR COLL STRATEGIC STUDIES
INST CARLISLE BARRACKS PA

General Hey've Captured our Hard Drive

2 NOV 1997 35 PAGES

PERSONAL AUTHORS: Nault, Mark

UNCLASSIFIED REPORT

ABSTRACT: (U) Joint Vision 2010 (JV 2010), an overview document describing the strategic vision of the Chairman of the Joint Chiefs of Staff (CJCS), was released in early 1997 and revealed a new joint armed forces battlespace concept called Full Spectrum Dominance. Information Operations (IO), which includes both Information Warfare (IW) and Command and Control (C2) doctrine, is the backbone of this emerging JV 2010 full spectrum dominance concept. Are there any significant strategic level IO concerns, for our military leaders who practice the strategic art in today's and tomorrow's joint armed forces, which ultimately delay or degrade the capabilities detailed in the new JV 2010? This author believes that the answer to this thesis question is a resounding YES! This Strategic Research Project (SRP) briefly reviews several basic, but recently updated, IO definitions, and describes the role that IO plays in the cyber missions depicted in the new JV 2010 and other related documents, such as the President's National Security Strategy (NSS), the Quadrennial Defense Review (QDR), the CJCS's National Military Strategy (NMS), as well as individual service concept documents.

DESCRIPTORS: *NATIONAL SECURITY, *DRIVES (ELECTRONICS), *INFORMATION WARFARE, COMPUTER PROGRAMS, THESES, COMMAND AND CONTROL SYSTEMS, JOINT MILITARY ACTIVITIES, MILITARY COMMANDERS, MILITARY TACTICS, STRATEGIC INTELLIGENCE.

AD-A341533

NAVAL POSTGRADUATE SCHOOL
MONTEREY CA

A High Resolution Satellite Communication Model

SEP 1997 133 PAGES

PERSONAL AUTHORS: Murphy, Brandee L.

UNCLASSIFIED REPORT

ABSTRACT: (U) Information warfare is a cornerstone of Joint Vision 2010 which addresses the future strategic environment for the United States. An integral component of information warfare is the continuing development of joint space doctrine. The Joint Warfare System (JWARS) is a large scale, systemic simulation being developed by the Joint Warfare Systems Office to aid in the evaluation of future joint doctrine and force structure. The purpose of this thesis is to develop and demonstrate simulation of Satellite Communications (SIMSATCOM), a high resolution, stochastic simulation of satellite communications for evaluating the effectiveness of message transmission and receipt by specified senders and receivers. SIMSATCOM is designed to operate as a stand alone simulation, but may be adopted as a high resolution module for a large scale simulation such as JWARS. The thesis describes SIMSATCOM in detail and provides analyses of simulation runs for different jamming levels and channel capacities.

DESCRIPTORS: *SATELLITE COMMUNICATIONS, *MESSAGE PROCESSING, *INFORMATION WARFARE, COMPUTERIZED SIMULATION, COMMUNICATIONS TRAFFIC, MILITARY DOCTRINE, THESES, HIGH RESOLUTION, ANTIJAMMING, COMMUNICATION SATELLITES, MILITARY SATELLITES, MULTICHANNEL COMMUNICATIONS.

AD-A340846

GENERAL ACCOUNTING OFFICE
WASHINGTON DC NATIONAL
SECURITY AND INTERNATIONAL
AFFAIRS DIV

Electronic Warfare: Test Results Do Not Support Buying More Common Sensor Systems

MAR 1998 11 PAGES

UNCLASSIFIED REPORT

ABSTRACT: (U) We have completed our follow-up review of the Intelligence and Electronic Warfare Common Sensor (IEWCS) program, which is to provide the Army and the Marine Corps with improved signals intelligence capability. In 1995, we suggested the Army's fiscal year 1996 IEWCS procurement request be reduced because operational testing to prove the system worked properly was not scheduled until fiscal year 1997. In 1996, we reported the Army had prematurely committed to low-rate production the prior year and recommended that additional IEWCS production planned for fiscal year 1997 be canceled. In response, the Department of Defense (DoD) reduced the number of systems to be procured, but permitted the Army to proceed. To assist the Congress in its oversight of DoD's management of systems acquisitions, we conducted this follow-up review to determine whether results of testing conducted since our previous review support continued IEWCS production.

DESCRIPTORS: *MILITARY INTELLIGENCE, *ELECTRONIC WARFARE, *SIGNALS, TEST AND EVALUATION, DEPARTMENT OF DEFENSE, MARINE CORPS, DETECTORS, ACQUISITION, PRODUCTION, OPERATIONAL EFFECTIVENESS, ARMY PROCUREMENT.

AD-A340087

ARMY WAR COLL
CARLISLE BARRACKS PA

Information: A Selected Bibliography

FEB 1998 41 PAGES

UNCLASSIFIED REPORT

ABSTRACT: (U) Information: A selected bibliography was compiled to support one of the special themes of the U.S. Army War College's curriculum. Focusing primarily on information warfare and operations, it also includes citations for other contemporary information issues such as information technology, information management, and the information highway. All references are dated 1995 to the present. Items listed in this bibliography are available in the U.S. Army War College Library collection. For your convenience, we have added our call numbers at the end of each entry. Please keep in mind that call numbers may vary from library to library.

DESCRIPTORS: *BIBLIOGRAPHIES, *ARMY, *INFORMATION WARFARE, WARFARE, DATA MANAGEMENT, INFORMATION SYSTEMS, EDUCATION, COMPUTERS, UNIVERSITIES, LIBRARIES, INTERNET, INFORMATION SCIENCES.

AD-A337392

ARMY COMMUNICATIONS-ELECTRONICS
COMMAND FORT MONMOUTH NJ

Command, Control, Communications, Computers, Intelligence & Electronic Warfare and Sensors and Information Management (C4IEWS&IM), Project Book, Fiscal Year 1998

1998 345 PAGES

UNCLASSIFIED REPORT

ABSTRACT: (U) This document displays a cross section of the Army Team's systems and equipment which are currently in development, production, or in the field. This publication reflects a coordinated effort between CECOM, PEO Command, Control and Communications Systems (PEO C3S), PEO Intelligence and Electronic Warfare & Sensors (PEO IEW&S), and PEO Standard Army Management Information Systems (STAM IS). The C4IEWS&IM military community shares the critical mission of equipping, sustaining, and modernizing technologically superior and integrated C4IEWS&IM systems. This mission supports the nation's warfighters in the accomplishment of dominant maneuver, precision engagement, full dimensional protection and focused logistics through information superiority.

DESCRIPTORS: *MILITARY INTELLIGENCE, *COMMAND CONTROL COMMUNICATIONS, *ELECTRONIC WARFARE, *DATA MANAGEMENT, DETECTORS, PRODUCTION, INFORMATION SYSTEMS, SIZES (DIMENSIONS), ARMY PERSONNEL, COMPUTERS, TEAMS (PERSONNEL), MISSIONS, CROSS SECTIONS, PROTECTION.

AD-A337178

SOUTHWEST RESEARCH INST
SAN ANTONIO TX

Information Warfare Modeling I

OCT 1997 46 PAGES

PERSONAL AUTHORS: Collier, Mark

UNCLASSIFIED REPORT

ABSTRACT: (U) This report documents the results of survey task in which the contractor was asked to identify current Information Warfare (IW) modeling development within the Department of Defense (DoD) and recommend an approach for IW modeling. It involved working with Rome Laboratory to identify their primary interest area in IW modeling, surveying DoD for ongoing unclassified IW modeling efforts, and defining an IW modeling architecture which Rome Laboratory could use in the future to guide research and development.

DESCRIPTORS: *COMPUTERIZED SIMULATION, *ELECTRONIC WARFARE, *INFORMATION WARFARE, DEPARTMENT OF DEFENSE, COMMAND AND CONTROL SYSTEMS.

AD-A336966

AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH SCHOOL OF ENGINEERING

A Modeling and Simulation Approach to Characterize Network Layer Internet Survivability

DEC 1997 194 PAGES

PERSONAL AUTHORS: King, Leif S.

UNCLASSIFIED REPORT

ABSTRACT: (U) The Air Force Core Competency of Information Superiority will be achieved in an age of decreasing AF manpower and corporate expertise. Increased AF reliance on COTS solutions, coupled with nearly ubiquitous points of entry to communication networks, create unique challenges in maintaining the Information Superiority edge. The protection of the internet is part of this equation. The internet supports the daily business traffic of the Air Force. Personnel, finance, and supply data flow through its routers. Controlling an adversary's access to our Information Systems, either the data, or the hardware and software that control the data and transform it into information, is a key operation of Defensive Information Warfare which is the primary focus in maintaining Information Superiority. This research will attempt to answer the viability of implementing measures designed to ensure the survivability of the internet communications infrastructure against denial of service attacks. It will provide planners the information to make decisions based on the cost and benefit tradeoffs associated with such measures.

DESCRIPTORS: *COMPUTER GATEWAYS, *DATA PROCESSING SECURITY, *INTERNET, *INFORMATION WARFARE.

AD-A336852

OFFICE OF THE SECRETARY OF THE ARMY WASHINGTON DC

Joint Technical Architecture - Army; Version 5.0

11 SEP 1997 182 PAGES

UNCLASSIFIED REPORT

ABSTRACT: (U) One of the underlying tenets of information age warfare is that shared situation awareness, coupled with the ability to conduct continuous operations, will allow information age armies to observe, decide, and act faster, more correctly and more precisely than their enemies. This presupposes that information is reliable, timely, available, usable, and shared. The underlying information infrastructure must, therefore, facilitate rather than inhibit the flow of information between sustaining base agencies and strategic tactical force elements and provide the flexibility to accommodate different missions and organizational structures. A Technical Architecture (TA) is a set of building codes. By itself it builds nothing. However, used in conjunction with the other enterprise architectures the operational and systems architectures the adoption and enforcement of the TA fosters interoperability between systems, as well dramatically reducing cost, development time, and fielding time for improved systems.

DESCRIPTORS: *INTEROPERABILITY, *COMPUTER ARCHITECTURE, *INFORMATION WARFARE, MILITARY REQUIREMENTS, DATA MANAGEMENT, INFORMATION EXCHANGE, COMPUTER COMMUNICATIONS, JOINT MILITARY ACTIVITIES, STANDARDS, SYSTEMS ANALYSIS, MILITARY PUBLICATIONS, SYSTEMS MANAGEMENT.

AD-A336481

NATIONAL DEFENSE INDUSTRIAL ASSOCIATION ARLINGTON VA

Proceedings of the Ninth Annual Special Operations/Low Intensity Conflict (SO/LIC) Symposium and Exhibition, "National Security Strategy in Transition" the Critical Role of Special Operations Forces (SOF) in Preparing Now for an Uncertain Future

19 FEB 1998 674 PAGES

UNCLASSIFIED REPORT

ABSTRACT: (U) Major topics of this symposium include: (1) A National Security Strategy for a New Century, (2) National Military Strategy of the United States of America, (3) Preparing Now for an Uncertain Future, (4) The Nature of Future Military Operations, (5) Transforming SOF for the 2020 Environment, (6) PSYOP and Information Operations-Integration and Interface, (7) SOF Aviation, (8) Civil Affairs Challenges of Post-Conflict Transitions in Failed Societies, (9) C4I: War in the Information Age for SOF, (10) Weapons Systems Modernization: The Future Demands Better, and (11) Waging Peace: SOF's Role in Peace Operations.

DESCRIPTORS: *MILITARY STRATEGY, *NATIONAL SECURITY, *MILITARY PLANNING, *SPECIAL OPERATIONS FORCES, MILITARY INTELLIGENCE, COMMAND CONTROL COMMUNICATIONS, MILITARY REQUIREMENTS, SYMPOSIA, JOINT MILITARY ACTIVITIES, WAR GAMES, MILITARY MODERNIZATION, PSYCHOLOGICAL WARFARE, NATIONAL DEFENSE, LOW INTENSITY CONFLICT, PEACEKEEPING, INFORMATION WARFARE.

AD-A334778

DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

Operational Requirements Document for the Unmanned Aerial Vehicle (UAV) Tactical Control System (TCS) Version 3.0

1996 10 PAGES

UNCLASSIFIED REPORT

ABSTRACT: (U) The requirement relates to the Office for the Under Secretary of Defense (Acquisition and Technology) Mission Areas 212 (Indirect Fire Support), 217 (Land Warfare Surveillance and Reconnaissance), 223 (Close Air Support and Interdiction), 227 (Air Warfare Surveillance and Reconnaissance), 232 (Amphibious, Strike, and Antisurface Warfare), 237 (Naval Warfare Surveillance and Reconnaissance), 322 (Tactical Intelligence and Related Activities (TIARA) for Tactical Land Warfare), 345 (Tactical Communications), 370 (Electronic Combat) and 373 (Tactical Surveillance, Reconnaissance, and Target Acquisition). The Tactical Control System (TCS) is the software, software-related hardware and the extra ground support hardware (antennae, cabling, etc.) necessary for the control of the Tactical Unmanned Aerial Vehicle (TUAV), and Medium Altitude Endurance (MAE) UAV, and Future Tactical UAVS. The TCS will also provide connectivity to identified Command, Control, Communications, Computers , and Intelligence (C4I) systems. TCS will have the objective capability of receiving High Altitude Endurance (MAE) UAV payload information. Although developed as a total package, the TCS will have the capability to be configured and down-scaled to meet the user's deployability or operator limitations.

DESCRIPTORS: *MILITARY REQUIREMENTS, *REMOTELY PILOTED VEHICLES, *TACTICAL COMMUNICATIONS, COMPUTER PROGRAMS, ELECTRONIC WARFARE, LAND WARFARE, CONTROL SYSTEMS, ACQUISITION, CLOSE SUPPORT, COMBAT SURVEILLANCE, TARGET ACQUISITION, MILITARY VEHICLES, INTERDICTION, AIRBORNE, AERIAL WARFARE.

AD-A333391

RAND CORP SANTA MONICA CA

In Athena's Camp; Preparing for a Conflict in the Information Age

1997 516 PAGES

PERSONAL AUTHORS: Arquilla, John; Ronfeldt, David

UNCLASSIFIED REPORT

ABSTRACT: (U) We have been posing our ideas about conflict in the information age for some years now, beginning in 1991 with our original ruminations about cyberwar, then about netwar, and lately about 'information strategy.' With each step, we have kept returning to a favorite set of themes; organization is as crucial as technology in understanding the information revolution; this revolution is giving rise to network forms of organization; and the rise of networks will continue to accrue power to nonstate actors, more than to states, until states adapt by learning to remold their hierarchies into hybrids that incorporate network design elements. Meanwhile, we have kept our eyes on emerging trends in conflict from the end of the Persian Gulf War, through recent developments in places like Chechnya and Chiapas to further our understanding that the context and conduct of conflict is changing from one end of the spectrum to the other. New modes of war, terrorism, crime, and even radical activism are all these emerging from similar information age dynamics? If so, what is the best preparation for responding to such modes? When the subject is warfare, for example, it is common wisdom that militaries tend to prepare for the last war, and there is much historical evidence to support this notion.

DESCRIPTORS: *THREAT EVALUATION, *MILITARY PLANNING, *INFORMATION WARFARE, MILITARY HISTORY, MILITARY STRATEGY, NATIONAL SECURITY, COMPUTER NETWORKS, MILITARY TACTICS, ELECTRONIC SECURITY, TERRORISM.

AD-A333373

NAVAL POSTGRADUATE SCHOOL
MONTEREY CA

Modeling Organizational Configuration and Decision Processes for Information Warfare Analysis

MAR 1997 142 PAGES

PERSONAL AUTHORS: Black, Bruce J.

UNCLASSIFIED REPORT

ABSTRACT: (U) For an organization to survive it must be able to adapt to its environment. A military organization operates in an environment that is constantly changing. The ability to model organizational configurations and organizational decision processes can assist the commander in adapting to the environment and understanding how a military organization is susceptible to Information Warfare (IW) attacks. First a commander must understand the concepts of Information Warfare, Command and Control and the concept of organizational decision processes and how these permit an organization to adapt to its environment. Then the commander must determine what level of detail is necessary to model the organizational decision processes for its environment. Next the commander must analyze his model for configuration and decision processes. Using such commercially available software as Organizational Consultant and VDT the commander can identify any organizational misfits to the environment and the IW attack susceptibilities of the organizational decision processes. In the end, this approach demonstrates that it is feasible to model organizational configuration and organizational decision processes in an information warfare environment.

DESCRIPTORS: *DECISION MAKING, *INFORMATION WARFARE, COMPUTER PROGRAMS, CONFIGURATIONS, COMMAND AND CONTROL SYSTEMS, MILITARY ORGANIZATIONS.

AD-A333216

NAVAL POSTGRADUATE SCHOOL
MONTEREY CA

An Information Security Education Initiative for Engineering and Computer Science

1 DEC 1997 31 PAGES

PERSONAL AUTHORS: Chin, Shiu Kai; Irvine, Cynthia E.; Frincke, Deborah

UNCLASSIFIED REPORT

ABSTRACT: (U) This paper puts forward a case for an educational initiative in information security at both the undergraduate and graduate levels. Its focus is on the need for such education, the desired educational outcomes, and how the outcomes may be assessed. A basic thesis of this paper is that the goals, methods, and evaluation techniques of information and computer security are consistent with and supportive of the stated goals of engineering education and the growing movement for outcomes based assessment in higher education.

DESCRIPTORS: *JOB TRAINING, *DATA PROCESSING SECURITY, *COURSES (EDUCATION), SOFTWARE ENGINEERING, DATA MANAGEMENT, SKILLS, CRYPTOGRAPHY, COMPUTER COMMUNICATIONS, COMPUTER ARCHITECTURE, COMPUTER NETWORKS, TRAINING MANAGEMENT, CONDITIONING (LEARNING), INFORMATION WARFARE.

AD-A332446

DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

Information Warfare: New Roles for Information Systems in Military Operations

3 DEC 1997 20 PAGES

PERSONAL AUTHORS: Crawford, George A.

UNCLASSIFIED REPORT

ABSTRACT: (U) In the past decade we have witnessed phenomenal growth in the capabilities of information management systems. National security implications of these capabilities are only now beginning to be understood by national leadership. Information Warfare (IW) is one of the new concepts receiving a great deal of attention inside the Washington DC beltway; in some circles IW is even touted as the cornerstone of future U.S. military doctrine. There is no doubt IW is a concept the modern military officer should be familiar with, for advancements in computer technology have significant potential to dramatically change the face of military command and control. Information warfare theory has tremendous political, technical, operational and legal implications for the military. This article seeks to define IW for the layman and discuss its potential applications. It will also attempt to identify potential military uses of existing information systems technology and address some of the issues facing those who will be responsible for implementing this new doctrine.

DESCRIPTORS: *MILITARY OPERATIONS, *INFORMATION SYSTEMS, *COMMAND AND CONTROL SYSTEMS, INFORMATION WARFARE, MILITARY PERSONNEL, NATIONAL SECURITY, LEADERSHIP, DATA MANAGEMENT, MILITARY DOCTRINE, COMPUTERS, INFORMATION THEORY, OFFICER PERSONNEL.

AD-A331946

AIR COMMAND AND STAFF COLL
MAXWELL AFB AL

Information Warfare: Planning the Campaign

APR 1996 78 PAGES

PERSONAL AUTHORS: Okello, Fredrick; Ayers, Richard; Bullock, Patrice; Erhili, Brahim; Harding, Bruce

UNCLASSIFIED REPORT

ABSTRACT: (U) Information warfare is a nebulous concept, but widely cited as a keystone in any future campaign. Even though information warfare has been used for centuries, current doctrine, policies, and guidance provide little help for the warrior to understand first, what information warfare is, and secondly, how to do it. "Information Warfare: Planning the Campaign" provides a logical approach for the information warrior to employ in planning for this aspect of warfare. This paper addresses the: (1) Current state of information warfare policy and doctrine, (2) Modeling of a system to identify its critical nodes and links, (3) Modeling of a Joint Forces Air Component Commander (JFACC) to serve as an example, (4) Examples of current and potential offensive and defensive information warfare tools used in information encounters, and finally, and (5) A step-by-step approach to information warfare campaign planning. Analysis of information and its flow is a daunting undertaking in all but the most simple of organizations. To remedy this, one can view the organization as a system and employ a model which will help illustrate information flows.

DESCRIPTORS: *COMPUTER ARCHITECTURE, *INFORMATION WARFARE, COMMAND CONTROL COMMUNICATIONS, WARFARE, INTEGRATED SYSTEMS, SYSTEMS ENGINEERING, INFORMATION SYSTEMS, INFORMATION TRANSFER, MILITARY DOCTRINE, COMPUTER AIDED MANUFACTURING, UNCONVENTIONAL WARFARE.

AD-A331679

NAVAL POSTGRADUATE SCHOOL
MONTEREY CA DEPT OF OPERATIONS
RESEARCH

Stochastic and Deterministic Models of Targeting, with Dynamic and Error-Prone BDA

SEP 1997 41 PAGES

PERSONAL AUTHORS: Baver, Donald P.; Jacobs, Patricia A.

UNCLASSIFIED REPORT

ABSTRACT: (U) Deep precision strike is a generic military operation that depends importantly on C4/ISR system contributions. Information from the latter is realistically subject to chance influences: targets are found and correctly identified generally at rates proportional to their numbers, locations, and activities, and to the coverage of shooter-serving sensors; the events of detection are realistically random, as are the delays, results, outcomes, and follow-up of the targeting shooters. In this paper a simplified version of the above complicated process is analyzed mathematically, here as a multi-stage queuing process with imperfect service. The probabilistic outcomes can be used to anticipate the results of higher-resolution simulations; these often are far more time consuming both to set up and run. Aspects of the above queuing situations can also be deduced via a deterministic 'fluid' queuing approximation that gives an adequate and convenient representation of aspects of the state variables and various measures of effectiveness in the stochastic queuing model. Relying on that agreement, we have elsewhere generalized the stochastic queuing model setup to fluid models that incorporate omitted realities, such as losses from target-list tracking, and the inevitable time dependencies, non-stationarities, and adaptive behaviors that typically occur in actual military operations or vignettes.

DESCRIPTORS: *MATHEMATICAL MODELS, *QUEUEING THEORY, *BATTLE MANAGEMENT, MILITARY INTELLIGENCE, COMMAND CONTROL COMMUNICATIONS, COMBAT EFFECTIVENESS, STOCHASTIC PROCESSES, DAMAGE ASSESSMENT.

AD-A331354

ARMY COMMAND AND GENERAL STAFF
COLL FORT LEAVENWORTH KS SCHOOL
OF ADVANCED MILITARY STUDIES

Information Operations - A New Tool for Peacekeeping

22 MAY 1997 92 PAGES

PERSONAL AUTHORS: Phillips, Gary E.

UNCLASSIFIED REPORT

ABSTRACT: (U) This monograph discusses the application of information operations to improve the efficiency and effectiveness of peace missions ranging from peacekeeping to peace imposition. Using a variety of models and an examination of the components of information operations this monograph demonstrates the applicability of these operations to peace missions. Examples from recent history provide a backdrop for evaluating previous applications and investigating other potential uses of information operations to support peace missions. Based on the validation of applicability the possible increase in effectiveness and efficiency are postulated and potential resource savings evaluated. The monograph first examines the status of international relations as a result of the demise of the Soviet Union and the rise of information technology. The impact of these two earthshaking events have forever changed the face the world.

DESCRIPTORS: *PEACEKEEPING, *INFORMATION WARFARE, MILITARY INTELLIGENCE, MILITARY FORCES (UNITED STATES), MILITARY HISTORY, INFORMATION EXCHANGE, INTERNATIONAL RELATIONS.

AD-A329719

AIR FORCE INST OF TECH
WRIGHT-PATTERSON AFB OH

Information Warfare: Few Challenges for Public International Law

26 SEP 1997 56 PAGES

PERSONAL AUTHORS: Meader, Gerald H.

UNCLASSIFIED REPORT

ABSTRACT: (U) Information Warfare is of rising concern a threshold question is, "why address this issue at all?" It deserves a look because our increasing dependence on information and information technologies makes us ever more vulnerable to this attractive, elegant weapon. Dependence on the National Information Infrastructure according to a recent report by a Defense Science Board Task Force, the information infrastructure of the United States is increasingly vulnerable. Indeed, because the U.S. is so very dependent on information technology, it is one of the most vulnerable nations to IW attack. This vulnerability extends to infrastructures related to military C4I, oil and gas control, water supply, government operations, mass media, civil emergency services, transportation control, finances (national and global), and production, inventory and process controls. They are vulnerable because all of these systems use increasingly complex, interconnected network control systems. These infrastructures are also interdependent such that an attack on one could have a cascade effect on others.

DESCRIPTORS: *INTERNATIONAL LAW, *INFORMATION WARFARE, TERRORISTS, ELECTRONIC WARFARE, NATIONS, UNITED STATES, CONTROL SYSTEMS, VULNERABILITY, SENSITIVITY, COMMUNICATION AND RADIO SYSTEMS, COMPUTER NETWORKS, PSYCHOLOGICAL WARFARE, LAW ENFORCEMENT, MASS MEDIA, FEDERAL LAW, INFRASTRUCTURE.

AD-A329699

NAVAL POSTGRADUATE SCHOOL
MONTEREY CA

Organizational Innovation and Redesign in the Information Age: The Drug War, Netwar, and Other Lower-End Conflict

AUG 1997 218 PAGES

PERSONAL AUTHORS: Berger, Alexander

UNCLASSIFIED REPORT

ABSTRACT: (U) The end of the Cold War and the rise of the Information Age have fostered an uncertain security environment which the United States is struggling to master. The purpose of this thesis is to explore the factors that lead complex organizations to initiate large-scale structural change in the face of environmental uncertainty, and more specifically to determine how the rise of the Information Age may change the organizational requirements of the U.S. national security structure. This thesis creates a unique framework for analysis, blending principles of organization and innovation theory with the theory of information-based 'netwar.' This study analyzes the organizational structures adopted by several transnational drug cartels, and compares them to that of U.S. counternarcotics forces. Next, this thesis reviews a series of recent occurrences pertaining to national security to test whether there are manifestations of netwar threats emerging, and whether new and old organizational actors are learning to adapt their structures to gain an advantage over the United States. Finally, this thesis is both predictive and prescriptive with regard to the issues of organizational redesign. It argues that structural changes are necessary for the United States to ensure the national security in an Information Age. Then it makes recommendations that would help the U.S. security structure redesign itself to become more agile in the face of Information Age threats.

DESCRIPTORS: *ORGANIZATIONS, *DRUG INTERDICTION, *OPERATIONS OTHER THAN WAR, MILITARY INTELLIGENCE, REQUIREMENTS, UNITED STATES, NATIONAL SECURITY, INFORMATION TRANSFER, SECURITY, THESES, NARCOTICS, INFORMATION WARFARE.

AD-A329064

ARMY SPACE AND STRATEGIC DEFENSE COMMAND HUNTSVILLE AL

BM/C3 Information Technology Distributed Processing and Information Warfare

1997 15 PAGES

PERSONAL AUTHORS: Hayes, J. L.; Merritt, Ira W.; Hayes, James C.; Mcfee, John K.; Sauer, Jon

UNCLASSIFIED REPORT

ABSTRACT: (U) The U.S. Army Space and Strategic Defense Command (USASSDC) Advanced Technology Directorate (ATD) currently manages several research programs that have the potential to significantly advance the current state of the art in information technology for future battle Management/Command, Control, and Communication (BM/C3) Systems. These programs address some of the challenges associated with full spectrum dominance in information warfare by providing new and innovative technologies for advanced distributed processing. The definition of information technology as it applies to BM/C3 is provided, as well as our vision for the future of distributed processing and its role in future BM/C3 systems. We propose that the realization of more effective BM/C3 systems utilizing megacomputer architectures to support the human in control will require continuing technological advances in high speed communications, architectural structures, automated decision support, modeling and simulation (M&S), and parallel processing algorithms.

DESCRIPTORS: *COMMAND CONTROL COMMUNICATIONS, *DISTRIBUTED DATA PROCESSING, *BATTLE MANAGEMENT, *INFORMATION WARFARE, ALGORITHMS, COMPUTER ARCHITECTURE, PARALLEL PROCESSING, PHOTONICS, THREAT EVALUATION, ARMY PLANNING, DECISION SUPPORT SYSTEMS.

AD-A328226

NAVAL WAR COLL NEWPORT RI

U.S. C4I and Logistics Vulnerabilities to Offensive Information Warfare

13 JUN 1997 31 PAGES

PERSONAL AUTHORS: Mckethan, Colton

UNCLASSIFIED REPORT

ABSTRACT: (U) The information revolution fostered by the microchip has made it possible for military commanders to receive information in unequaled quantity and quality. U.S. commanders have a broad range of opportunities resulting from digitized technologies that enhance of military equipment performance and the application of force. These information advances represent force enablers providing synergistic advantage to operational command and control (C2), intelligence, and logistic functions. However, there is a down side, in that the computers and microchips have vulnerabilities that must be addressed to retain operational force advantage. Information warfare is central to the way the nation plans to fight in the future, and information systems now connect U.S. military forces on a worldwide basis. Despite the enhancements that connectivity brings, with integration of global communications, state and non-state actors are provided new ways to access and undermine the C2, intelligence, and logistics function via computer and communication networks. This new area of vulnerability extends from the strategic, through the operational, down the tactical levels of warfare.

DESCRIPTORS: *INFORMATION SYSTEMS, *COMMUNICATIONS NETWORKS, DEPARTMENT OF DEFENSE, VULNERABILITY, CHIPS (ELECTRONICS), INTEGRATION, COMMAND AND CONTROL SYSTEMS, COMPUTER APPLICATIONS, DEFENSE PLANNING, DECEPTION, INTRUSION, GLOBAL COMMUNICATIONS, INFRASTRUCTURE.

AD-A327513

NAVAL WAR COLL NEWPORT RI

Off the Trodden Path: Thinking Through the Military Exploration of the Information Domain

21 FEB 1997 87 PAGES

PERSONAL AUTHORS: O'Connell, Ed

UNCLASSIFIED REPORT

ABSTRACT: (U) Trends in today's security environment point to a changed information domain on the horizon--a cyberspace of increased density, interconnectivity and collaboration, where links and nodes have disappeared. As military planners, we are stuck somewhere between institutional skepticism reserved for new tricks, and the awe and wonder with which the rest of our society views this new frontier. Yet, insights provided by recent strategic information warfare exercises suggest the military is beginning to approach cyberspace from a new perspective--as a place like any other. These trends and early insights will have profound implications for how we project force into this changed cyberspace of tomorrow.

DESCRIPTORS: *NATIONAL SECURITY, *COMPUTER NETWORKS, *MILITARY PLANNING, *INFORMATION WARFARE, DATA BASES, MILITARY REQUIREMENTS, COMPUTER COMMUNICATIONS, MILITARY APPLICATIONS, MAN COMPUTER INTERFACE.

AD-A327427

ARMY WAR COLL
CARLISLE BARRACKS PA

Information Operations: A Layman's Perspective

1 APR 1997 34 PAGES

PERSONAL AUTHORS: Bishop, Roy V.

UNCLASSIFIED REPORT

ABSTRACT: (U) The subject of Information Operations (IO), formerly called Information Warfare, is having a profound impact on the Department of Defense and the Armed Services because of the proliferation of information technologies throughout the Armed Services. Most literature on the subject will tell you that IO is the center piece for a larger revolution in military affairs. Whether these technological innovations represent a revolution or not, is of little importance in the grand scheme of things. But taking maximum advantage of their potential is. Utilization of these technologies is not without considerable risk. This paper examines where we got started with incorporating high technology into intelligence, weapons, and command, control, communications and computer systems, assess where we are and where we are going, discuss the associated vulnerabilities and what we are doing to protect against them.

DESCRIPTORS: *ELECTRONIC WARFARE, *INFORMATION EXCHANGE, WEAPONS, RISK, COMPUTERS.

AD-A327112

NAVAL RESEARCH LAB WASHINGTON DC VACUUM ELECTRONICS BRANCH

Christine: A Multifrequency Parametric Simulation Code for Traveling Wave Tube Amplifiers

5 MAY 1997 39 PAGES

PERSONAL AUTHORS: Antonsen, Thomas M., Jr.; Levush, Baruch

UNCLASSIFIED REPORT

ABSTRACT: (U) A model and computer code are presented that simulate the operation of traveling wave tube amplifiers (TWTs). The model is based on the well known parametric theory in which the relevant properties of the interaction circuit are the phase velocity and coupling impedance of the waves supported by the slow wave structure. The model includes a multifrequency description of both the fields of the structure and the space charge fields. This allows for the study of harmonic and intermodulation distortion. The beam is treated as an ensemble of disks with an effective axial velocity spread. Several options are available for specifying the parameters of the interaction circuit: using a sheath helix description, importing data from another model, or using data from experimental measurement. The advantages of the code are that it can relatively quickly simulate situations in which the amplifier is driven by multiple input frequencies, it is readily portable to different platforms, and it facilitates tube design by enabling users to vary parameters relatively easily.

DESCRIPTORS: *TRAVELING WAVE TUBES, *INTERMODULATION, FREQUENCY, ELECTRONIC WARFARE, PARAMETRIC ANALYSIS, COMPUTER PROGRAMMING, DISKS, ELECTRICAL IMPEDANCE, SPACE CHARGE, SLOW WAVE CIRCUITS, AMPLIFIERS, COUPLING CIRCUITS, PHASE VELOCITY.

AD-A327000

ARMY COMMUNICATIONS-ELECTRONICS COMMAND FORT MONMOUTH NJ

Advance Planning Briefing for Industry: Information Dominance for the Full Spectrum Force

29 MAY 1997 510 PAGES

UNCLASSIFIED REPORT

ABSTRACT: (U) The Army C4IEW is pleased to present these proceedings of the 1997 Advance Planning Briefing for Industry (APBI) entitled 'Information Dominance for the Full Spectrum Force.' The objective of this publication is to provide industry with a comprehensive overview of our research and development programs, sustainment efforts and corresponding contract opportunities available to industry within the next five years. Technology is the critical component to attaining full-spectrum operations. The Department of Defense must team with private industry at every opportunity in order to ensure advanced technologies for our forces in the 21st Century.

DESCRIPTORS: *COMMAND CONTROL COMMUNICATIONS, *ELECTRONIC WARFARE, *ARMY PLANNING, MILITARY INTELLIGENCE, DEPARTMENT OF DEFENSE, SYMPOSIA, ARMY RESEARCH, INDUSTRIAL RESEARCH, RESEARCH MANAGEMENT.

AD-A326646

ARMY WAR COLL
CARLISLE BARRACKS PA

The Role of the Intelligence Community in Preparing to Win the Information War

10 APR 1997 25 PAGES

PERSONAL AUTHORS: Mccollum, William W.

UNCLASSIFIED REPORT

ABSTRACT: (U) Increasing reliance on information-based technology is not unique to the United States, but growing awareness of the vulnerabilities created by this reliance has focused attention on protecting our information and information systems, while the potential value of offensive information operations, particularly in peacetime, has been less fully explored. This paper examines the relationship between defensive and offensive information warfare, looks at the status of governing policies and doctrine, discusses the vital role of intelligence in winning the defensive and offensive information war, and makes recommendations regarding organizing the intelligence community to support the successful prosecution of the offensive information war.

DESCRIPTORS: *MILITARY INTELLIGENCE, *NATIONAL SECURITY, *VULNERABILITY, *INFORMATION THEORY, MILITARY OPERATIONS, WARFARE, UNITED STATES, POLICIES, DEFENSE SYSTEMS, PEACETIME, INFORMATION SYSTEMS, AWARENESS.

AD-A326536

ARMY WAR COLL STRATEGIC STUDIES
INST CARLISLE BARRACKS PA

Information Warfare - Who is Responsible? Coordinating the Protection of Our National Information Infrastructure

3 MAR 1997 42 PAGES

PERSONAL AUTHORS: Thompson, Michael J.

UNCLASSIFIED REPORT

ABSTRACT: (U) The government of the United States relies on the information superhighway, officially known as the National Information Infrastructure (NII), to pass critical information. Banking, transportation, communication, medicine, electrical power, and manufacturing are also dependent upon the NII to pass the information required for them to operate. The U.S. Military depends on the NII for the movement of personnel and equipment, voice and data communications and research and development. The nation's power is provided through the national power grid which is connected to the NII. The NII is vulnerable to intrusion, disruption and exploitation by hackers, hostile entities, or anyone with a modest amount of automation equipment. Leadership at the national level is required to coordinate government and private sector actions to ensure the security and reliability of the NII.

DESCRIPTORS: *MANAGEMENT INFORMATION SYSTEMS, *DATA PROCESSING SECURITY, *COMPUTER NETWORKS, MILITARY INTELLIGENCE, ELECTRONIC WARFARE, DEPARTMENT OF DEFENSE, INFORMATION TRANSFER, COMPUTER COMMUNICATIONS, VULNERABILITY, COMMAND AND CONTROL SYSTEMS.

AD-A326368

ARMY WAR COLL
CARLISLE BARRACKS PA

Defensive Information Warfare in Today's Joint Operations: What's the Real Threat?

APR 1997 47 PAGES

PERSONAL AUTHORS: Ashman, Bruce W.

UNCLASSIFIED REPORT

ABSTRACT: (U) Information Warfare (IW) is an emerging concept that affects the use of automated systems and reflects the growing realization that information technology can be used to gain an advantage over other users. Since the Gulf War, the incidents of information systems attacks have increased, especially in the civilian environment. Attacks against military systems have gone as far as penetrating sensitive, previously secure systems. As this threat against information or computer-based systems becomes more blatant, it raises the question of how vulnerable to attack are our automated military systems. Emerging technologies promise greater speed, accuracy and reliability for military operations while simultaneously producing greater lethality and situation awareness. However, as the Armed Forces depend more and more on these systems to perform routine and specialized operations, the risk of penetration, disruption, or even compromise becomes apparent. While information warfare has great potential as a valid offensive tool, this paper explores the threat to unified and joint military operations from a defensive information warfare perspective.

DESCRIPTORS: *DATA PROCESSING SECURITY, *JOINT MILITARY ACTIVITIES, DATA BASES, MILITARY INTELLIGENCE, COMMAND CONTROL COMMUNICATIONS, ELECTRONIC WARFARE.

◆**AD**-A325529

NAVAL WAR COLL NEWPORT RI

Critical Factors in Cyberspace

7 FEB 1997 23 PAGES

PERSONAL AUTHORS: Van Cleave, John

UNCLASSIFIED REPORT

ABSTRACT: (U) Since WWII, warfare and conflict involving the United States, has taken on an antiseptic dimension. Conflicts have been resolved in far away places, separated by distance and a powerful military force able to project power and take the fight to the enemy. In doing so the U.S. has remained relatively immune to attacks on its own social, economic, political, and military infrastructures. But as the U.S. forges ahead into the information age, the global connectivity inherent in this transformation also brings about new vulnerabilities. The vast advantages of space the fabled high ground including the civil and military capabilities it brings to the U.S will soon be overshadowed by what could be termed the common ground, cyberspace. In cyberspace highly computerized and networked social, economic, political, and military infrastructures become intertwined, increasing their vulnerability to attack. This paper will explore some current and future challenges that must be considered carefully as we develop the new common ground in cyberspace and the impact that cyber weapons will have in reshaping operational and strategic planning. It will also identify critical factors traditional in U.S. infrastructures that are increasingly vulnerable to attack through cyberspace due to these new linkages.

DESCRIPTORS: *COMMAND CONTROL COMMUNICATIONS, *DATA PROCESSING SECURITY, *MILITARY CAPABILITIES, *MILITARY PLANNING, SOFTWARE ENGINEERING, LOGISTICS SUPPORT, INFORMATION EXCHANGE, STRATEGIC ANALYSIS, VULNERABILITY, COMPUTER PROGRAM VERIFICATION, INTERNET.

◆ Included in the DTIC Review, March 2000

AD-A325003

NAVAL WAR COLL NEWPORT RI

Information Warfare and its Impact on National Security

13 JUN 1997 20 PAGES

PERSONAL AUTHORS: Devries, Anita D.

UNCLASSIFIED REPORT

ABSTRACT: (U) For years, the United States national security posture has relied heavily on secured sea lines of communication, friendly borders, unmatched human and material resources, unlimited mobilization capability, and nuclear hegemony. This paper defines information warfare; examines its offensive and defensive components; explores potential threats, information warfare legalities and nature; and concludes that we face a tremendous challenge at the strategic level to keep our current status of being a world power to be reckoned with.

DESCRIPTORS: *WARFARE, *NATIONAL SECURITY, ELECTRONICS, GLOBAL, STRATEGY, DEFENSE SYSTEMS, IMPACT, INFORMATION SYSTEMS, THREATS, MOBILIZATION, COMPUTERS, VULNERABILITY, TELECOMMUNICATIONS, MILITARY TACTICS, INFRASTRUCTURE.

AD-A324333

ARMY COMMAND AND GENERAL STAFF COLL FORT LEAVENWORTH KS SCHOOL OF ADVANCED MILITARY STUDIES

Heavy Division Organic Signals Intelligence (SIGINT): Added Value or Added Baggage

13 DEC 1996 69 PAGES

PERSONAL AUTHORS: Taylor, Robert J., Jr

UNCLASSIFIED REPORT

ABSTRACT: (U) This monograph discusses heavy division organic SIGINT and its limited ability to aid the commander in the division's fight. Modern weapon system employment demands that intelligence and SIGINT provide precision intelligence at extended ranges. Furthermore, tactical SIGINT system mobility and survivability requires carriers that are as mobile and survivable as the combat systems they support. This monograph examines the range, accuracy of collection, and the mobility and survivability of tactical SIGINT systems. The monograph first determines that the changing nature of the modern battlefield and doctrine require tactical SIGINT assets to adequately range targets, determine precisely their location, move with combat formations yet remain survivable. The monograph uses these three requirements through each section as a guide in determining the value of SIGINT. Next, it evaluates tactical SIGINT through two case studies. The first is Desert Shield/Desert Storm and the second is at the National Training Center. Both case studies evaluate currently available tactical SIGINT systems.

DESCRIPTORS: *MILITARY INTELLIGENCE, *ELECTRONIC WARFARE, *TACTICAL WARFARE, *TACTICAL INTELLIGENCE, *ELECTRONIC INTELLIGENCE, MILITARY OPERATIONS, MOBILITY, IRAQ, KUWAIT, SURVIVABILITY, BATTLEFIELDS, WEAPON SYSTEMS.

AD-A316760

NATIONAL DEFENSE UNIV
WASHINGTON DC INST FOR
NATIONAL STRATEGIC STUDIES

Defensive Information Warfare

AUG 1996 82 PAGES

PERSONAL AUTHORS: Alberts, David S.

UNCLASSIFIED REPORT

ABSTRACT: (U) The problem of defending against information warfare is real. Our citizens and the organizations that provide them with the vital services they need can find no sanctuary from these attacks. The low cost of mounting these attacks has enlarged the field of potential adversaries and complicated efforts to collect intelligence and array our defenses. The consequences of a well-planned and coordinated attack by a relatively sophisticated foe could be serious. Even the threat of such an attack or digital blackmail is a distinct possibility. How the public will respond to the threat of IW infrastructure attacks or to actual attacks is unclear, but is a major determinant of future policy and actions. This situation is getting worse with the rapid proliferation of information technology and know-how. We are becoming increasingly dependent on automation in every aspect of our lives. As information technology becomes an essential part of the way organizations and individuals create products and provide services, the need for interconnectivity and interoperability increases. With this increased need for exchanges of information (and products), vulnerabilities increase. Finally, the increased reliance on commercial-off-the-shelf products or commercial services makes it more and more difficult for organizations and individuals to control their own security environment.

DESCRIPTORS: *WARFARE, *STRATEGIC ANALYSIS, *THREAT EVALUATION, *DEFENSE PLANNING, *INFORMATION SCIENCES, MILITARY INTELLIGENCE, NUCLEAR PROLIFERATION.

AD-A314073

RAND CORP SANTA MONICA CA

The Advent of Netwar

1996 127 PAGES

PERSONAL AUTHORS: Arquilla, John; Ronfeldt, David

UNCLASSIFIED REPORT

ABSTRACT: (U) This briefing elucidates a concept-'netwar'-that we mentioned in an earlier article on 'cyberwar.' Whereas the latter term refers primarily to information-based military operations designed to disrupt an adversary, netwar relates to lower-intensity conflict at the societal end of the spectrum. In our view, netwar is likely to be the more prevalent and challenging form of conflict in the emerging information age and merits careful and sustained study. In terms of conduct, netwar refers to conflicts in which a combatant is organized along networked lines or employs networks for operational control and other communications. The organizational forms that netwar actors adopt may resemble 'stars' that have some centralized elements, or 'chains' that are linear, but the major design will tend to be 'all-channel' networks in which each principal node of an organization can communicate and interact with every other node. Further, netwar actors may develop hybrid structures that incorporate elements of some or all of the above designs in varied ways. Strong netwar actors will have not only organizational, but also doctrinal, technological, and social layers that emphasize network designs. Netwar actors may make heavy use of cyberspace, but that is not their defining characteristic-they subsist and operate in areas beyond it.

DESCRIPTORS: *ELECTRONIC WARFARE, *COMPUTER NETWORKS, CONTROL, CHAINS, MILITARY APPLICATIONS, HYBRID SYSTEMS, CENTRALIZED, EVOLUTION (DEVELOPMENT).

AD-A313366

DECISION SCIENCE CONSORTIUM INC
FALLS CHURCH VA

Decision Support for Battlefield Planning

MAR 1996 37 PAGES

PERSONAL AUTHORS: Lehner, Paul E.; Tolcott, Marvin A.

UNCLASSIFIED REPORT

ABSTRACT: (U) As part of a research program investigating decision support capabilities for battlefield planning, an examination was made of developmental systems in each of five principal elements of Army C2I: maneuver control, fire support, air defense, intelligence and electronic warfare, and combat support services. The systems described generally fall into two categories (with some overlap): (1) decision support systems that attempt to capture automatic specific decision processes, usually employing advanced technologies such as artificial intelligence; and (2) decision aids that attempt to enhance human cognition in command decision making, usually based on psychological research findings. These efforts appear to be mainly driven by technology, rather than being based on systematic study of operational requirements and there is little evidence of their operational use. Another type of support, not reviewed, takes the form of application programs that process data already available in management information systems; these are being built into C2I systems by the systems developers, and are therefore likely to find operational use. Increased emphasis on studying command decision making requirements is recommended.

DESCRIPTORS: *BATTLEFIELDS, *COMMAND AND CONTROL SYSTEMS, *ARMY PLANNING, *DECISION SUPPORT SYSTEMS, MILITARY INTELLIGENCE, AIR DEFENSE, ELECTRONIC WARFARE, MANEUVERABILITY, AUTOMATION, MANAGEMENT INFORMATION SYSTEMS, DECISION MAKING.

AD-A312146

ARMY WAR COLL
CARLISLE BARRACKS PA

Interoperability: The Cornerstone of Information Warfare

12 APR 1996 27 PAGES

PERSONAL AUTHORS: Barac, Gregory G.

UNCLASSIFIED REPORT

ABSTRACT: (U) Information warfare has won the joint acceptance within DoD and may become the biggest threat faced by our nation. The great achievement of interoperability between information-based systems (e.g., computers) also introduced inherent risks and vulnerabilities, which is the cornerstone of information warfare. Information warfare includes the ability to exploit and dominate information made assessable through computers and communications. Should there be concern about these vulnerabilities? Absolutely. Modern societies depend upon these information-based systems to live and work. This paper introduces the recentness of information warfare and highlights some current issues, like who is leading the effort. The success of the information society to make their systems interoperate with other systems greatly increased the potentiality of information warfare. A review of the evolution of system interoperability highlights this phenomenon. As a result of being directly influenced by the industrial-age society, leaders over the age of forty may be too challenged to adequately grasp the issues of information warfare and may lead ineffectively.

DESCRIPTORS: *INFORMATION SYSTEMS, *DATA PROCESSING SECURITY, *INTEROPERABILITY, *SECURE COMMUNICATIONS, COMPUTER COMMUNICATIONS, MILITARY APPLICATIONS, EVOLUTION (GENERAL), ACCEPTABILITY.

AD-A311887

NAVAL POSTGRADUATE SCHOOL
MONTEREY CA

Information Warfare: Implications for Forging the Tools

JUN 1996 160 PAGES

PERSONAL AUTHORS: Thrasher, Roger D.

UNCLASSIFIED REPORT

ABSTRACT: (U) One part of the modern Revolution in Military Affairs (RMA) is the possibility of a new form of warfare-often called information warfare. Development of information warfare depends on technological advances, systems development and adaptation of operational approaches and organizational structures. This thesis assesses the implications of information warfare for the technology and systems development areas, with the underlying motivation of ensuring the military is postured to win the information warfare RMA through effective research, development and acquisition. This assessment takes place primarily through a 'Delphi' process designed to generate discussion between selected information warfare experts about the impacts of information warfare. This thesis concludes that information warfare is largely dependent on commercial information technology. This dependence means the military should rely on the commercial sector for most technological advances and products-with government research funds focused on military-unique research areas. Use of commercial items, coupled with DoD standard architectures, may enable a decentralization of information warfare acquisition to the user level.

DESCRIPTORS: *ELECTRONIC WARFARE, *INFORMATION SYSTEMS, *MILITARY APPLICATIONS, INTEGRATED SYSTEMS, COMMERCE, DETECTORS, COMPUTER PROGRAMMING, COMPUTER ARCHITECTURE, DATA ACQUISITION, COMMERCIAL EQUIPMENT.

AD-A311885

NAVAL WAR COLL NEWPORT RI JOINT
MILITARY OPERATIONS DEPT

Reexamining the Principle of Surprise in 21st Century Warfare

16 JUN 1996 22 PAGES

PERSONAL AUTHORS: Baker, Virginia E.

UNCLASSIFIED REPORT

ABSTRACT: The U.S. military has undergone profound changes over the past decades, however the basic principles of warfighting, developed in the late 1900's, remain essentially unchanged. Nevertheless, as we continually revise doctrine and the way we fight wars, particularly in the approaching 21st Century, it is important to review the principles of war in the context of the current military environment. Probably the most affected by the technological and institutional changes in the military is the principle of surprise. Surprise, a vital force multiplier in any military operation, can achieve quick, decisive victory in battle. Therefore its employment will continue to be effective in 21st Century warfare; however commanders must consider the impact of changes in technology and intelligence on achieving surprise; and how secrecy, another vital component of surprise, will be more difficult to maintain in the future. The technological advantages of the United States is diminishing due to technology exchanges, commercial availability of military systems, and gray market activities. Good intelligence analysis is becoming more difficult to achieve in a complex real-time, multidiscipline collection environment. Massive infusions of information increase the fog and friction of war and commanders must quickly and accurately assess intelligence and take risks accordingly.

DESCRIPTORS: *OPERATIONAL EFFECTIVENESS, *MILITARY APPLICATIONS, *MILITARY MODERNIZATION, *MILITARY PLANNING, MILITARY INTELLIGENCE, MILITARY OPERATIONS, WARFARE, NATIONAL SECURITY, INFORMATION EXCHANGE, TECHNOLOGY TRANSFER, MILITARY DOCTRINE.

AD-A310529

NATIONAL AIR INTELLIGENCE CENTER
WRIGHT-PATTERSON AFB OH

Analysis of Protection of Electronic Information in the Gulf War

MAY 1996 22 PAGES

PERSONAL AUTHORS: Taiying, Lin

UNCLASSIFIED REPORT

ABSTRACT: (U) In the Gulf War in early 1991, the most lethal and most expensive weapons were not the guided missiles, fighter craft, tanks, or warships, but the electronic information system deployed by the multinational troops in the Gulf area led by the United States. This information system was large-scale, advanced in technology, strict in organization, and high in operational efficiency, providing the overall, precise, timely, and continuous information about Iraqi troops to the multinational troops in its various command structure levels. Thus, the demand for prescribing combat plans and command execution was ensured, to have key functions in winning the war. The Gulf War was a concentrated manifestation of the modern informationized battleground. In the view of the U.S. forces, the Gulf War signaled the conclusion of a combat era and marked the coming of the C3I era. Therefore, analysis on the electronic information protection system in this war is very important and significant to cope with combat in the future high-tech conditions.

DESCRIPTORS: *MILITARY INTELLIGENCE, *ELECTRONIC WARFARE, *INFORMATION SYSTEMS, *PROTECTION, *ELECTRONIC SECURITY, MILITARY FORCES (UNITED STATES), MILITARY HISTORY, IRAQ, FOREIGN TECHNOLOGY, DEFENSE SYSTEMS, MILITARY FORCES (FOREIGN), COMBAT SUPPORT, ELECTRONIC EQUIPMENT, OPERATIONAL EFFECTIVENESS, RUSSIAN LANGUAGE, TRANSLATIONS, DEFENSE PLANNING, CHINA, FOREIGN LANGUAGES.

AD-A309782

ARMY WAR COLL
CARLISLE BARRACKS PA

Information Warfare: The Organizational Dimension

FEB 1996 27 PAGES

PERSONAL AUTHORS: Minehart, Robert F., Jr

UNCLASSIFIED REPORT

ABSTRACT: (U) Since the December 1992 publication of the Department of Defense (DoD) classified directive on Information Warfare (IW) considerable effort has been expended examining this issue. Despite this attention, a clear vision for the implementation of IW within DoD and the U.S. Government as a whole has yet to emerge. Three pillars are essential to achieving a viable IW strategy and supporting architecture: policy doctrine, organization training and requirements/technology. Much has been written, discussed, and even debated on the need for overarching national policy in this area, as well as the multitude of capabilities and vulnerabilities stemming from our increased reliance on advanced technology. A similar focus on the organizational component of IW has not occurred. The study specifically addresses the role of organizations as a key component of IW. Both the progress achieved to date within DoD and the significant challenges remaining to be overcome at the interagency level are examined. Specific recommendations are provided on how better to organize the IW effort.

DESCRIPTORS: *MILITARY INTELLIGENCE, *COMMAND CONTROL COMMUNICATIONS, *ELECTRONIC WARFARE, *INFORMATION EXCHANGE, MILITARY REQUIREMENTS, POLICIES, ORGANIZATIONS, SIZES (DIMENSIONS), TRAINING, MILITARY DOCTRINE, VISION, ARCHITECTURE.

AD-A309400

ARMY WAR COLL
CARLISLE BARRACKS PA

Artificial Intelligence Applications to Information Warfare

22 MAR 1996 35 PAGES

PERSONAL AUTHORS: Kirk, David C.

UNCLASSIFIED REPORT

ABSTRACT: (U) In the coming years, a critical element of combat will likely be waged in the information infrastructure. Current strategic concepts do not compensate for the vulnerability of our ever-increasing information-based society. In this research project, artificial intelligence technology (specifically, intelligent agents) was explored. Intelligent agents were found to have characteristics that could help execute an information war. Although there still is work to be done, intelligent agents may someday manage the information flow, be the core technology in network firewalls, and contribute to overall network security through continuous red team vulnerability assessments.

DESCRIPTORS: *NATIONAL SECURITY, *DATA MANAGEMENT, *ARTIFICIAL INTELLIGENCE, MILITARY STRATEGY, INFORMATION EXCHANGE, VULNERABILITY, COMPUTER NETWORKS, INFRASTRUCTURE.

AD-A307334

NAVAL WAR COLL NEWPORT RI JOINT MILITARY OPERATIONS DEPT

The Challenge of Netwar for the Operational Commander

6 MAR 1996 30 PAGES

PERSONAL AUTHORS: Poole, James A.

UNCLASSIFIED REPORT

ABSTRACT: (U) The threat of intrusions to U.S. domestic and military infrastructure and information systems is very real and may affect our national security now and in the future. Information has become a new center of gravity that must be protected. Netwar is one tool of information warfare that the operational commander can use in defensive and offensive operations to gain information dominance. Netwar targets military or civilian non-weapons computer networks to gain a military advantage while it protects one's own systems from attack. With an overview of netwar concepts, this paper explores the benefits of netwar for the commander, the defensive and offensive decisions that must be made, and some prescriptions for the future that will enable the commander to fight and win conflicts effectively in the twenty-first century.

DESCRIPTORS: *NATIONAL SECURITY, *DATA PROCESSING SECURITY, *COMPUTER NETWORKS, WARFARE, DECISION MAKING, DEFENSE SYSTEMS, INFORMATION SYSTEMS, TOOLS, ATTACK, PROBLEM SOLVING, COMMAND AND CONTROL SYSTEMS, DOMESTIC, MILITARY COMMANDERS, INTRUSION, INFRASTRUCTURE.

DTIC Review Order Form

MAIL Orders:
DTIC-BRR
Defense Technical Information Center
8725 John J. Kingman Rd., Ste 0944
Ft. Belvoir, VA 22060-6218

CALL-IN Orders:
DTIC-BRR
Defense Technical Information Center
(703) 767-8274/(DSN) 427-8274
1-800-225-DTIC (3842)
(Menu selection 1, Option 1)

FAX Orders:
DTIC-BRR
Defense Technical Information Center
(703) 767-9070/(DSN) 427-9070

INTERNET Orders:
msorders@dtic.mil
or
www.dtic.mil/dtic/docorderform.html

Requesting Organization Information

User Code __|__|__|__|__|__|__

Organization ______________________________

Point of Contact ______________________________

Phone Number ______________________________

Method of Payment

Note: All Credit Card Types Must Be Preregistered

□ **Deposit Account Number** __|__|__|__|__|__-__|__

□ **VISA** □ **MasterCard** □ **American Express**

Account Number ______________________________

Cardholder's Name ______________________________

Expiration Date ______________________________

DTIC does not accept cash, checks, or COD.

Service Codes

R - Regular Service
Priority Services (Must be called in or faxed)
P - Picked Up Next Business Day ($10.00 surcharge/document)
M - Mailed Next Business Day ($10.00 surcharge/document)
E - Express - Mailed Next Business Day (Guaranteed Delivery in 2 Business Days) ($20.00 surcharge/document)

Document Orders

Service Code	AD Number	Quantity Hard Copy	Quantity Microfiche
	/JAA		
	/JAA		
	/JAA		
	/JAA		
	/JAA		
	/JAA		
	/JAA		
	/JAA		
	/JAA		
	/JAA		
	/JAA		
	/JAA		
	/JAA		
	/JAA		
	/JAA		